Смотреть на отзывы и не использовать общедоступный WI-FI – эксперты Новосибирска рассказали, как обезопасить себя в интернете

18.07.2024

Эксперты круглого стола обсудили распространенные способы обмана в интернете и борьбы с ними, поделились мерами защиты и статистическими данными.

В России с каждым годом растет количество случаев правонарушений и число обманутых граждан с использованием интернета. Этой теме уделяется особое внимание в правоохранительных органах и организациях разных сфер.

> «Если 10 лет назад преступления в интернете находились в пределах статистической погрешности от количества всех преступлений, то сейчас они составляют около 40%. И доля интернет-преступлений с каждым годом растет», – рассказал представитель МВД Слабухо Михаил.

Благодаря мерам профилактики интернет-мошенничеств и увеличению мер безопасности количество преступлений удается сократить.

На платформе «Авито» количество жалоб клиентов на противоправные действия сократилось в 100 раз за четыре года. Уровень доверия граждан повысился на

12%, всего 73% россиян доверяют сервису. Этому способствует ряд разработанных новшеств внутри платформы: безопасный мессенджер, защита номера пользователей, проверки персональных данных и реальности объекта продажи, системы искусственного интеллекта, контролирующие контент, а также разработанные обучающие материалы.

Еще одно направление работы «Авито» — повышение качества сервиса и прозрачности пользователей.

> «Нам важно, чтобы покупатели могли легко найти на платформе хороших продавцов. Для этого мы даем рекомендации о том, как еще улучшить поведение и поощряем продавцов с высоким уровнем сервиса. В числе факторов влияющих на это — верификация, которая позволяет убедиться, что за профилем стоит конкретный человек или компания», — отметила Наталья Юматова.

Телекоммуникационные сервисы в качестве профилактической работы запускают информационные ролики в салонах продаж и повышают уровень проверки данных при обращении пользователей. Не прошедшие проверку пользователи блокируются, чтобы с таких сим-карт не удалось совершить сомнительные операции.

> «С 2022 года Теле2 разработало свою систему, которая позволяет определять подмену номера. Также все операторы подключены к единой системе Роскомнадзора, которая владеет исходными данными принадлежности номера. На основе этих баз мы определяем около 1,2 млн мошеннических смс, которые поступают абонентам, и более 1 млн вызовов. Все они блокируются и не доходят до абонентов», — рассказал руководитель департамента продаж и клиентского сервиса макрорегиона «Сибирь» Tele2 Евгений Корешков.
>
> «Чтобы злоумышленники не завладели данными абонента, введена двухфакторная аутентификация, пароль приходит на привязанную электронную почту. При замене сим-карты введены дополнительные меры, абонент при обращении должен предоставить свой паспорт, если обращается не он, обязательно должна быть нотариальная доверенность, которая проверяется на соответствующем сайте, тогда услуга оказывается не день в день. После замены сим-карты на сутки блокируются смс-сообщения. Это сделано для того, чтобы избежать рассылки смс от лица пользователя, в случае если сим-карту восстановил мошенник», — прокомментировал Корешков Евгений.

При покупке сим-карты меры безопасности также усилены: в случае отсутствия паспортных данных в анкете абонента, через 7 дней она будет заблокирована, продавцам такой сим-карты также грозит ответственность. Количество проданных сим-карт ограничено пятью штуками для одного человека, в том числе на разных точках продажи.

Злоумышленники часто звонят от имени банков, поэтому внутри банковской сферы разработана собственная система безопасности. Используется двухфакторная

аутентификация, которая позволяет подтвердить личность клиента при попытке входа в интернет-банк. Подобная проверка проходит при обращении в колл-центр. Дополнительно пользователям направляют памятки, разрабатывают игровые форматы обучения безопасности в интернете.

> «80% успеха – это профилактика, поэтому в интернет-ресурсах в рамках квестов и квизов для школьников мы рассказываем о популярных схемах обмана. Например, банки никогда не звонят в мессенджерах, сотрудники Центрального банка также не могут звонить, так как учреждение не работает с физическими лицами. Большой пласт посвящен блоку мошенничества в социальных сетях и предложениям об удаленной работе, рассказываем о фишинговых сайтах», – отметила начальник департамента безопасности банка «Уралсиб» Голубева Наталья.

Важным аспектов в борьбе с такими преступлениями является сотрудничество всех организаций, в том числе банков и сотовых операторов, а также бдительность самих граждан.

> «Чем быстрее мы получим информацию, тем выше будет вероятность раскрытия интернет-преступлений и быстрее вернуться денежные средства их законным владельцам. Поэтому мы регулярно проводим совещания с представителями сотовых операторов и банковской сферы. В целом ситуация улучшается, но есть над чем работать», – рассказал представитель прокуратуры Злобин Ярослав.
>
> «Иногда ответа от операторов приходится ждать до трех месяцев, – добавил Ярослав Злобин. – За это время денежные средства могут раствориться, их сложно будет найти и распутать цепочку мошеннической схемы».

Эксперты считают, профилактику мошенничеств стоит проводить начиная со школьного возраста, детям необходимо рассказывать о распространённых схемах, а также встречаться с представителями других учреждений, раздавать памятки и брошюры. Прокуратурой с начала года проведено более 400 таких мероприятий. Хорошим форматом для обучения безопасности в интернете являются игры и квизы.

Наталья Юматова отметила, что уровень цифровой грамотности пользователей со временем растет.

> «Этому способствует та просветительская работа, которую активно ведет крупный бизнес и правоохранительные органы. Люди все реже попадаются на простые уловки, но все еще подвержены манипуляциям с помощью социальной инженерии. Например, когда создается стрессовая ситуация или для убедительности используются утекшие ранее данные пользователя. Инструментом борьбы с явлением становятся более содержательные, например игровые, механики, через которые можно познакомить людей с более сложными сценариями и научить безопасному поведению в интернете».

Чтобы не стать не потерять деньги и данные , специалисты рекомендуют:

- При покупках в интернете проверять безопасность сайта. Этому свидетельствует протокол https и зеленая галочка в строке адреса.
- При заполнении данных карты на сайте не включать галочку «автозаполнение».
- Не оставлять без внимание телефон при включенных push-уведомлениях на заблокированном телефоне. Информация может оказаться доступна любому рядом находящемуся человеку.
- Не вводить персональные данные и платежные реквизиты с общедоступных компьютеров.
- Не вводить персональные данные, не оплачивать покупки при подключении в общедоступной сетке Wi-Fi.
- В случае смены номера телефона, уведомить об этом все банки и другие службы, чтобы обновить данные. В ином случае мошенники смогут восстановить старый номер телефона и получить доступ к паролю от сервисов через эсэмэс.
- Отслеживать операции в мобильных приложения, чтобы в случае необходимости зафиксировать факт мошенничества.
- Отключить переадресацию вызовов.
- Выбирать хорошо знакомые интернет-платформы и магазины. Крупные платформы внедряют инструменты защиты сделок и стремятся максимально обезопасить своих пользователей.
- Общение с продавцом следует вести только внутри защищенной платформы и не переходить в сторонние каналы коммуникации.
- Ориентироваться на среднюю рыночную цену выбранного товара или услуги. Если продавец предлагает цену сильно ниже рынка — это повод насторожиться и как минимум задать больше вопросов.
- При выборе продавца внимательно изучить его профиль: посмотреть историю сделок, почитать отзывы других покупателей. Не переводить предоплату, если знаете продавца недостаточно хорошо. По возможности выбирать продавца или исполнителя, который готов получить оплату по факту, или пользуйтесь сервисами «безопасной сделки».

Анастасия Новоселова