Эксперт рассказала о самых частых типах киберугроз в интернете

В первом квартале 2025 года фишинговые атаки с использованием искусственного интеллекта и вредоносные Android-приложения стали одними из самых серьёзных киберугроз. По словам Екатерины Едемской, инженер-аналитика компании «Газинформсервис», мошенники начали активно использовать нейросети для создания фальшивых электронных писем, которые выглядят абсолютно как настоящие. Такие письма, якобы от банков или работодателей, убедительно просят пользователей ввести свои логины и пароли, что приводит к утечкам данных. В 2024 году такие фишинговые атаки стали причиной около 20% всех утечек данных по миру.

Кроме того, значительную угрозу представляют поддельные Android-приложения, маскирующиеся под популярные программы, мессенджеры и игры. Мошенники используют их для кражи данных пользователей, и эти приложения, зачастую, бывают очень сложно отличимы от оригиналов. Как только такие приложения попадают на смартфон, они превращают его в «шпионский гаджет», давая злоумышленникам доступ к личной информации. Такие угрозы становятся все более сложными для обнаружения, что делает смартфоны уязвимыми для взлома.

Также в топ-угроз попали кибератаки на облачные сервисы и мобильных операторов связи. Хакеры пытаются получить доступ к личным данным, хранящимся на облачных платформах, чтобы использовать их для шантажа или атак на работодателей. Взлом баз данных телекоммуникационных компаний позволяет злоумышленникам манипулировать телефонными номерами, совершать несанкционированные списания средств, а также проводить более сложные атаки. Наряду с этим, злоумышленники активно использовали программы-вымогатели, которые теперь направлены не только на организации, но и на простых пользователей, требуя выкуп за расшифровку файлов.