# Жертвы мошенников в интернете

Стремительное развитие Интернета открыло новую платформу для торговли и общения, но в то же время позволило мошенникам использовать невинных людей в своих преступных целях. Недобросовестные преступники все чаще выбирают жертв в Интернете, забирая у ничего не подозревающих людей их деньги или персональные данные. Новый экономический анализ позволил выявить последствия таких мошенничеств для жертв с экономической точки зрения.

Наиболее распространенными видами интернет-мошенничества являются фишинг, вредоносное ПО, социальная инженерия, мошенничество с использованием интернет-банкинга и романтические аферы. Все они осуществляются в киберпространстве в различных формах, имеют разные целевые рынки и тактику. Например, фишинговые аферы связаны с тем, что человека обманом вынуждают предоставить конфиденциальную информацию, например, пароли или номера кредитных карт, а атаки вредоносных программ направлены на компьютеры или мобильные устройства пользователей, что позволяет преступникам получить доступ к персональным данным, удаленно хранящимся в киберпространстве. Социальная инженерия — это когда мошенник манипулирует человеком, заставляя его разгласить конфиденциальную информацию путем создания фальшивых личностей или апеллируя к человеческим эмоциям, таким как симпатия, доверие или страх. Романтические аферы могут включать в себя создание ложных отношений через Интернет либо для получения финансовой выгоды, либо в злонамеренных целях, например, для кражи личных данных.

С экономической точки зрения эти виды мошенничества могут иметь разрушительные последствия как в финансовом, так и в психологическом плане для тех, кто от них пострадал. В финансовом плане жертвы могут оказаться вынужденными платить мошенникам большие суммы денег, поскольку часто чувствуют себя вынужденными платить им напрямую после того, как их обманули с помощью тактики психологического манипулирования, использующей такие человеческие эмоции, как страх или сочувствие, что может затруднить рациональное поведение в подобных ситуациях без надлежащего руководства и поддержки со стороны до того, как они стали жертвами сетевых хищников.

Что еще более тревожно, так это то, насколько сложно это сделать в настоящее время, особенно с учетом того, что киберпреступность продолжает стремительно расти с каждым годом на всех платформах, охватывающих весь мир, что усложняет выявление любого злого умысла до участия в действиях, связанных с использованием цифровых средств, и делает его обнаружение на более позднем этапе еще более маловероятным, если только системные инструменты не оснащены средствами защиты, специально предназначенными для предотвращения эксплуатации. Для предотвращения возможного вторжения в сеть за ее стенами используются технологии искусственного интеллекта (AI), алгоритмы глубокого обучения и систематической обработки естественного языка (NLP), а для наблюдения за ними — надежные ресурсы, зарегистрированные официально, действующие профессионально и легально, предоставляющие надежные услуги круглосуточно.

В заключение, если вы собираетесь участвовать в деятельности в Интернете, то делайте это с осторожностью, поскольку за экранами компьютеров находятся реальные люди, ежедневно совершающие преступления против невольных жертв, которые стоят невинным людям времени и энергии, а также драгоценных ресурсов, истощая одновременно активы пострадавших сторон (как материальные, так и нематериальные, физические/виртуальные), что существенно влияет на жизнь пострадавших независимо от их географического местонахождения в зависимости от характера.