



Потерпевшими от киберпреступлений являются граждане абсолютно всех категорий, включая как социально-незащищенные слои населения (инвалиды, пенсионеры, несовершеннолетние), так и люди, занимающие руководящие посты в организациях (предприятиях) всех форм собственности, имеющие несколько высших образований.

В ходе совершения преступлений злоумышленники используют звонки с номеров, визуально приближенных к номерам телефонов правоохранительных органов, служб банков (например, звонки на WhatsApp с номера +900, 900, тогда как официальный номер Сбербанка 900).

На сегодняшний день набирает популярность среди мошенников реализация преступных схем с использованием искусственного интеллекта. Используемые мошенниками схемы постоянно меняются, «подстраиваясь» под общественно-политическую обстановку, значимые события в государстве. Так, в Сибирском федеральном округе в 2024 году совершено 15 437 краж и 46 925 фактов мошенничества с использованием информационно-телекоммуникационных технологий (компьютерная техника и средств мобильной связи). Вашему вниманию представлены наиболее распространенные способы совершения киберпреступлений.

Обман под видом предложений от известных компаний и «Подмена мерчанта (продавца)»

Злоумышленники создают фишинговые ресурсы для хищения данных и денежных средств, имитируя страницы крупных компаний, интернет-магазинов. Жертве предлагается приобрести товар, услугу по скидке или поучаствовать в акции. Для привлечения жертвы используют контекстную рекламу, рассылку в менеджерах.

Поддельные штрафы

Мошенники имитируют уведомления от органов исполнительной власти о якобы имеющихся штрафах, задолженностях. Соответствующие сведения направляют в адрес электронной почты и предлагают произвести оплату перейдя по ссылке из фишингового письма. Рассчитывая заплатить штраф или погасить задолженность, жертва переходит по ссылке и вводит данные банковской карты в мошенническую форму оплаты.

Обман на площадках бесплатных объявлений (Avito и др.) и маркетплейсах

В большинстве случаев жертва сама входит в контакт с мошенниками в чате на сайте объявлений или маркетплейсах для покупки товара. В ходе общения злоумышленники предлагают продолжить переписку в мессенджере для уточнения деталей или доставки товара. Мошенники запрашивают у жертвы ФИО, адрес, номер телефона для заполнения формы доставки. Жертву вынуждают перейти по ссылке на заранее сгенерированный фишинговый ресурс, который имитирует официальные страницы курьерских служб, после введения банковских реквизитов списываются средства.

Криптоскам, псевдоброкеры, финансовые пирамиды

Широко получившая последнее время схема, в результате использования которой причиняется наиболее крупный ущерб – заработок на бирже, заманивание прибыльными инвестициями, в том числе в криптосфере. Преступниками создается максимальная видимость того, что общение происходит с представителями крупной инвестиционной площадки, их сайты имеют видимое сходство с банковскими организациями (например, Газпром-инвестиции, РБК-инвестиции, Тинькофф-инвестиции и т.д.), назначается личный брокер, общение с которым может осуществляться даже посредством видеозвонков. Под их руководством создается якобы личный кабинет на торговой площадке, в котором отображаются все внесенные денежные средства, и прибыль. Однако их дальнейший вывод невозможен.