

УДК 343.72

ВИДЫ МОШЕННИЧЕСТВА В ИНТЕРНЕТЕ*Е. А. Кудравец**курсант 2 курса**Академии МВД Республики Беларусь**Научный руководитель: И. А. Шаматульский,**заместитель начальника кафедры расследования преступлений**следственно-экспертного факультета**Академии МВД Республики Беларусь,**кандидат юридических наук, доцент*

Нельзя преуменьшать роль информационно-коммуникационных технологий в жизни человека, общества и государства. Невозможно представить современную жизнь без использования компьютеров, телефонов и иных средств коммуникации. Отличительной особенностью общения при помощи современных информационно-коммуникационных технологий является его анонимность, чем активно пользуются злоумышленники. Одним из наиболее распространенных видов преступлений, совершаемых в Интернете, являются хищения, в частности мошенничества. По данным МВД Республики Беларусь, только за начало 2022 года было совершено около 1 200 интернет-преступлений [1].

Мошенничество в Интернете имеет различные виды, информированность о которых необходима в деятельности сотрудников правоохранительных органов. В наше время можно выделить следующие виды мошенничества с использованием информационно-коммуникационных технологий:

1. Мошенничества, связанные с интернет-магазинами. Зачастую такие преступления совершаются на крупных торговых площадках: Kufar, Avito, Ebay и других. Как правило, мошенники публикуют объявление о продаже товара, значительно занижая его цену и запрашивают предоплату за товар при помощи денежных средств на банковскую карту, указанную в объявлении. Также стоит отметить, что в таких объявлениях отсутствует услуга самовывоза или курьерской доставки, а также полная информация о продавце.

2. Фишинг. При осуществлении данного вида мошенничества злоумышленник/злоумышленники от имени банков рассылают гражданам электронные письма, содержащие ссылки на фишинговые сайты, на которых предлагается ввести реквизиты банковской карты, после чего эти данные становятся доступны злоумышленнику.

3. Вишинг. Данный вид мошенничества также называется голосовой фишинг. При осуществлении такого способа совершения мошенничества злоумышленник звонит гражданину, представляясь сотрудником банка с целью

завладения реквизитами его банковской карты или убеждая перейти по фишинговым ссылкам, которые должны будут прийти на номер потерпевшего [2].

1. Предлагают перейти по ссылкам. Что делать, если атакуют интернет-мошенники? [Электронный ресурс]. URL: <https://ctv.by/predlagayut-pereyti-po-ssylkam-chto-delat-esli-atakuuyut-internet-moshenniki?ysclid=lct5lkibhg891491461> (дата обращения: 12.01.2023). [Вернуться к статье](#)

2. Следственный комитет предупреждает о мошенниках в мессенджерах [Электронный ресурс]. URL: <https://www.belta.by/incident/view/sledstvennyj-komitet-preduprezhdaet-o-moshennikah-v-messendzherah-425131-2021/?ysclid=lct5tgs22591200920> (дата обращения: 12.01.2023). [Вернуться к статье](#)