

АДМИНИСТРАЦИЯ ГОРОДА ЧЕЛЯБИНСКА  
**КОМИТЕТ ПО ДЕЛАМ ОБРАЗОВАНИЯ ГОРОДА ЧЕЛЯБИНСКА**

ул. Володарского, д. 14, г. Челябинск 454080 тел/факс: (8-351)700-18-01, E-mail: edu@cheladmin.ru

25 СЕН 2023      № 10/12693  
На № \_\_\_\_\_ от \_\_\_\_\_

Руководителям учреждений

О направлении информации

С целью информационно-разъяснительной работы направляем в Ваш адрес письмо ГУ МВД России по Челябинской области от 01.09.2023 № 1/12693 «О новых видах мошенничества, совершаемых с использованием ИТ-технологий.

Данную информацию прошу довести до всех заинтересованных лиц.

Приложение на 2 л. в 1 экз.

Председатель Комитета

С.В. Портве

И.Г. Мужагитова

700-18-25

Разослать: в МКУ ЦОДОО, СП МКУ ЦОДОО, МБУ ДПО ЦРО (для рассылки всем ОУ).



М В Д Р о с с и и

Г Л А В Н О Е У П Р А В Л Е Н И Е  
М И НИСТЕРСТВА ВНУТРЕННИХ ДЕЛ  
Р О С С И Й С К О Й Ф Е Д Е Р А Ц И И  
П О Ч Е Л Я Б И Н С К О Й О Б Л А С Т И  
(ГУ МВД России по Челябинской области)

ул. Елькина, 34, Челябинск, 454091  
Тел. Факс. № (351) 267-72-34

01.09.2023 № 1118693  
на № от

О направлении информации

Министру информационных  
технологий, связи и цифрового  
развития Челябинской области

И.Б. Фетисову

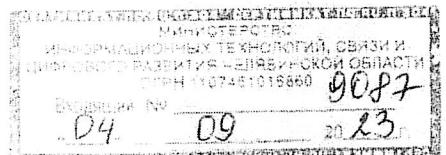
Уважаемый Игорь Борисович!

ГУ МВД России по Челябинской области информирует о появлении новых видов мошенничества, совершаемых с использованием IT-технологий:

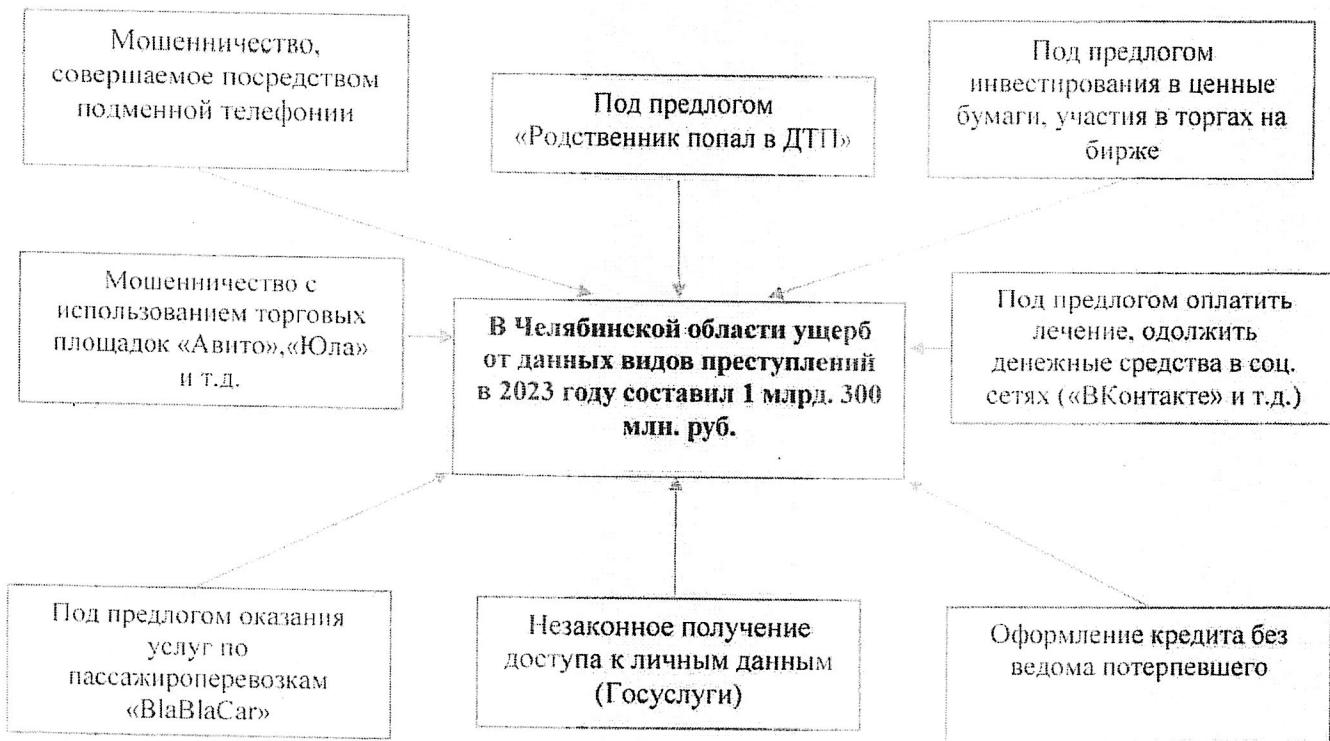
1. Сайты, имитирующие ресурсы государственных ведомств и справочных систем. Мошенники размещают шаблоны документов, которые обычно ищут в Интернете бухгалтеры, секретари, сотрудники, занимающиеся налоговой или финансовой деятельностью. Шаблоны документов при этом заражены вирусами. Когда сотрудник скачивает документ, на его компьютере запускается программа удаленного доступа. С ее помощью мошенники меняют в договорах компаний банковские реквизиты, чтобы затем получить на свои счета деньги, предназначенные подрядчикам и заказчикам.

2. Мошенники, представляясь сотрудниками банка, предлагают установить на смартфон «официальное сертифицированное» приложение финансовой организации для проверки устройства и поиска уязвимостей. Далее злоумышленники отправляют потенциальным жертвам ссылку на фишинговый сайт с инструкцией по установке приложения. После установки приложения мошенники получают удаленный доступ к смартфону и выводят денежные средства из онлайн-банка клиента.

3. Сообщения от якобы Федеральной службы судебных приставов. Мошенники направляют гражданам электронные письма и сообщения об имеющейся задолженности, угрожая внести должника в «федеральный реестр недобросовестных плательщиков», заблокировать его счета (банковские карты). Чтобы этого избежать, необходимо пройти по поступившей ссылке для погашения имеющейся задолженности. После перехода по ссылке, денежные средства перечисляются на счета мошенников.



Помимо указанных способов мошенничества, наиболее используемыми схемами дистанционных мошенничеств на территории Челябинской области являются:



Информация о наиболее распространенных способах мошенничества с использованием ИТ-технологий может быть применена для проведения информационно-просветительской работы в трудовых коллективах и создания информационного контента.

*С.Н. Соколов*  
Заместитель начальника –  
начальник полиции

И.В. Белецкий