

**УПРАВЛЕНИЕ ОБРАЗОВАНИЯ АДМИНИСТРАЦИИ
ОЗЕРСКОГО ГОРОДСКОГО ОКРУГА ЧЕЛЯБИНСКОЙ ОБЛАСТИ**

Уральская ул., д.8, г. Озерск Челябинской области, 456780

Телефон/факс (35130) 7-19-62

E-mail: obrazovanie@gorono-ozersk.ru

17.02.2025 № 2501-30/257
На _____ от _____

Руководителям образовательных
организаций

О направлении информации

Уважаемые руководители!

В соответствии с письмом Министерства информационных технологий, связи и цифрового развития Челябинской области от 10.02.2025 г. № 1601/699, направляю Вам для сведения и использования в информационно-разъяснительной работе обновленные информационные материалы Главного Управления МВД России по Челябинской области (по итогам 2024 года) от 03.02.2025 № 1/1419 о наиболее распространенных схемах хищения денежных средств, совершаемых с использованием информационно-коммуникационных технологий.

Приложение: на 2 л. в 1 экз.

Начальник Управления

Е.В. Волегова

Мишенкова Наталья Николаевна
8 (351-30) 5-78-22

Рассылка: дело, исполнитель, ОО



МВД России

**ГЛАВНОЕ УПРАВЛЕНИЕ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
по ЧЕЛЯБИНСКОЙ ОБЛАСТИ
(ГУ МВД России по Челябинской области)**

Министру информационных
технологий, связи и цифрового
развития Челябинской области

Фетисову И.Б.

ул. Елькина, д. 34, г. Челябинск, 454091
тел. (351) 267-72-34

03.02.2025

1/1419

№

на №

от

О направлении информации

03.02.2025

1601-200/965

Уважаемый Игорь Борисович!

За 12 месяцев 2024 года в Челябинской области ущерб от преступлений, совершенных с использованием информационно-коммуникационных технологий составил 3 млрд. 714 млн. руб. ГУ МВД России по Челябинской области¹ информирует о наиболее распространенных ИКТ – преступлениях²:

1. Мошенничество под предлогом инвестирования в ценные бумаги и криптовалюту, при котором злоумышленники представляются финансовыми брокерами и заманивают граждан «исключительными» предложениями, возможностью получения высокого дохода, используя названия крупных нефте-газодобывающих компаний и холдингов, таких как «Binance», Газпроминвести, ТинькоффИнвест, вынуждают потерпевшего вносить крупные суммы без возможности дальнейшего вывода денежных средств. Потерпевшие: все категории граждан независимо от пола, образования, экономического, национального, социального статуса, а также возраста.

2. Мошенничество, при котором злоумышленники представляются сотрудниками кредитно-финансовых учреждений и правоохранительных органов, используя методы психологического воздействия и пользуясь доверчивостью граждан, вынуждают потерпевших сообщать персональные данные, сведения о финансовом состоянии и информацию о наличии автотранспорта в собственности. Затем под манипулятивным воздействием мошенников потерпевшие переводят денежные средства на якобы безопасные расчетные счета (в отдельных случаях переводят деньги, вырученные от срочной продажи автотранспорта, недвижимости, сделку по срочной продаже имущества организуют сами мошенники). Потерпевшие: все категории граждан, независимо

¹ Далее – «ГУ МВД».

² Преступления в сфере компьютерной информации и (или) совершаемые с использованием информационно-коммуникационных технологий.

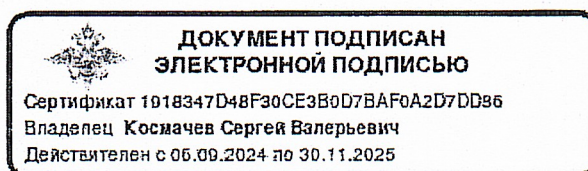
от пола, образования, экономического, национального, социального статуса, а также возраста.

3. Мошенничество под предлогом взломанной учетной записи на портале Государственных услуг, при котором злоумышленники, маскируясь под представителей операторов связи, убеждают потенциальную жертву, что срок действия SIM-карты истек. Под предлогом продления договора на обслуживание абонентского номера злоумышленники просят сообщить код из СМС. На самом деле это оказывается код для входа в личный кабинет на портале «Госуслуги». После того как мошенники получают код, они входят в учетную запись, меняют контрольный вопрос и оставляют сообщение о блокировке аккаунта и необходимости позвонить по указанному номеру. Войдя в учетную запись, мошенники могут оформить кредит на потерпевшего, получить налоговый вычет, продать данные или же собрать информацию о гражданине с целью дальнейшего «адресного психологического давления»³.

Информация о наиболее распространенных схемах совершения преступлений может быть использована при организации информационно-разъяснительной работы в трудовых коллективах, разработке адресного информационного контента.

Начальник

С.В. Космачев



Исп. С.Н. Соколов
Тел. (351)267-72-60

³ Адресное психологическое давление — процесс сбора данных, предварительной подготовки и использования эмоциональных триггеров, направленных на конкретного человека.