ИНФОРМАЦИЯ
МО МВД России «Ханты-Мансийский»

За период времени с 01.03.2026 года по 31.03.2026 года, в ДЧ МО МВД России «Ханты — Мансийский», зарегистрированы 72 сообщений и заявлений, о совершенных преступлениях, на территории города Ханты - Мансийска и района, по которым возбуждены уголовные дела. Из которых:

- 21 фактов преступлений, совершены неизвестными лицами, путем оформления на имена заявителей договора займов, в различных микро кредитных организациях, путем использования вредоносных программных обеспечении, в следствии перехода заявителями по неизвестным ссылкам и предоставления кодов подтверждений, либо путем использования старых абонентских номеров, по которым остался цифровой след прежних пользователей;

- 3 факта преступлений, совершены путем тайного хищения денежных средств со счета банковской карты заявителя, в следствии утраты самой банковской карты заявителем;

- 7 фактов преступлений совершены неизвестным лицом, путем тайного хищения денежных средств со счетов банковских карт заявителей, в результате использования неизвестным лицом, вредоносных программных обеспечений, вредоносных ссылок, сообщения кодов подтверждений заявителями.

- 6 фактов преступлений, совершены группой неизвестных лиц с распределенными ролями, в результате звонков или сообщений в мессенджерах, действующих по схеме: Получают от заявителя коды подтверждения, под любым предлогом — Далее от имени службы безопасности, сообщают о несанкционированном доступе в «Госуслуги» так как был сообщен код неизвестным лицам — Далее переводят разговор на сотрудника «ЦБ РФ», который сообщает о якобы поступивших заявках на оформление кредитных договорах, либо о попытках переводов денежных средств на Украину от имени заявителя, которые необходимо срочно предотвратить — Далее, для большего убеждения о выполнении требований якобы сотрудников ЦБ РФ, по видео связи, связывается мнимый сотрудник ФСБ или сотрудники иных структур, убеждая в том, что правоохранительными органами осуществляется проверка, а так же убеждают в соблюдении конфиденциальности, в ходе которого запрещается кому либо сообщать о происходящем под угрозой, в случае не соблюдения, о привлечении заявителя к ответственности, в связи с пособничеством — Далее, после полного убеждения пострадавшего, вновь сотрудник «ЦБ РФ» дает различные указания, по блокировке всех банковских счетов и переводе, имеющихся на счетах сбережений, на «Безопасный» банковский счет Центрального банка. Указания о якобы «декларировании» ценного имущества, путем продажи и перевода денежных средств с продажи на «Безопасный» счет ЦБ. Указания об оформлении кредитных договоров, и

переводе полученных кредитных средств на «Безопасный» счет ЦБ.

- 3 факта совершенных преступлений, путем списания денежных средств со счетов банковских карт заявителей, через различные маркетплейсы, такие как «Вайлдберриз», «Озон», «Яндексмаркет».

- 7 фактов совершенных преступлений, в ходе которых, неизвестное лицо использует сайты бесплатных объявлений, таких как «Авито» или страницы социальных сетей, таких как «Вконтакте», и под предлогом продажи или покупки товаров, путем обмана завладевают денежными средствами.

- 18 фактов совершенных преступлений, в ходе которых, неизвестные лица, по средствам вредоносных программных обеспечении, вредоносных ссылок, или получения кода подтверждения в ходе звонка, получают доступ к компьютерной информации охраняемой законом, а именно путем взлома личного кабинета портала «Госуслуги».

- 5 фактов совершенных преступлений, под предлогом дополнительного заработка на биржевом рынке, используя поддельные сайты торговых площадок.

- 3 факта совершенных преступлений, в ходе которых заявителям от имени знакомых, в различных мессенджерах поступают сообщения с просьбой занять денежные средства на короткий срок.

При проведении профилактических мероприятий с гражданами проживающих на территории Ханты - Мансийского района, мало вещать о уже совершенных мошеннических действиях в отношении других граждан. При проведении профилактики, необходимо акцентировать и доводить до граждан следующие обстоятельства:

- Предоставление какого - либо кода подтверждения, осуществляется только в ходе личного присутствия в какой - либо организации, при необходимости, например в отделении банка при обслуживании сотрудником банка запрашивается код. В ходе телефонных звонков, никакими службами или организациями, коды подтверждения, для совершения каких - либо операций, не запрашиваются. Если код подтверждения запрашивается по инициативе неизвестного лица, без предшествующих действий владельца, необходимо прекратить контакт с данным лицом.

- Звонки сотрудниками портала «Госуслуги», с уведомлениями о подозрительной активности в личном кабинете, никогда не совершаются, лишь поступают уведомления по электронной почте с официального адреса: no-reply@gososlugi.ru, если поступают с иных адресов, это мошенники! В случае, если к личному кабинету не привязан адрес электронной почты, поступают уведомления посредством СМС сообщений от контакта подписанного как «gosuslugi» без отражения абонентского номера, так как мошенники под видом «Госуслуг», отправляют уведомления о подозрительной активности в виде обычного СМС сообщения от неизвестного абонентского номера.

- Сотрудники Центрально банка РФ, не работают с физическим

лицами и не осуществляют звонки с целью предотвращения мошеннических действий и не просят осуществлять переводы на безопасный счет.

- Звонки от любых сотрудников правоохранительных органов, осуществляются только для вызова граждан, в соответствующий территориальный орган, для выяснения обстоятельств по возникшим вопросам. Либо обговариваются альтернативные способы для личной встречи. Звонки по видеосвязи сотрудниками правоохранительных органов не осуществляется. Сведения о совершении какого — либо присутствия, фиксируется только в ходе личного присутствия заявителя или свидетеля.

- При поступлении сообщений, в различных мессенджерах от имени друзей, родственников или знакомых, с просьбой пройти голосование по ссылке или открыть какой — либо закрепленный файл формата .APK (установочное приложение), необходимо, прежде всего, осуществить звонок данному человеку по мобильной связи и уточнить сведения о поступившем сообщении. Так как в подобных ссылках или файлах, спрятано вирусное ПО, посредством которых злоумышленники получают доступ к сотовым телефоном после перехода или попытки открытия файла.

- При поступлении сообщений, в различных мессенджерах, от имени друзей, родственников или иных знакомых, с просьбой осуществления займа денежных средств на короткий период, необходимо лично осуществить звонок, по мобильной связи данному человеку, с целью уточнения действительности данной просьбы. Так как аккаунты друзей, знакомых и родственников, могут быть взломаны злоумышленниками.

- При осуществлении покупок в сети интернет, необходимо пользоваться только проверенными интернет ресурсами. Иные интернет ресурсы или сообщества, где отражена цена интересующего товара, на много ниже рыночной, чаще все является мошенническими.

- В случае, когда граждане перестают пользоваться абонентским номером, при переходе на другого оператора или смене номера, которым пользовались длительное время, прежде чем перейти на другой номер, необходимо предыдущий, отвязать от личных кабинетов различных интернет ресурсов, которые находились в пользовании, в первую очередь от мобильных банков и сайтов МКК. Так как, после прекращения использования абонентским номером, чаще всего в течении 6 месяцев, сотовый оператор в одностороннем порядке расторгает договор оказания услуг связи и перерегистрирует на другого пользователя, при этом чаще всего остается цифровой след от предыдущего пользователя, в виде привязок в различных интернет ресурсах, чем пользуются злоумышленники, целенаправленно приобретая подобные абонентские номера.