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

18 ОКТ 2023 № 07/8473

На № _____ от _____

Директору МКУ «ЦОДОО г.Челябинска»
Сычевой А.А.

Начальникам СП МКУ «ЦОДОО г.Челябинска»

Руководителям образовательных учреждений

Уважаемые руководители!

Направляем для руководства и использования в работе письмо Главного Управления Министерства внутренних дел Российской Федерации по Челябинской области о появления новых видов мошенничеств, совершаемых с использованием IT-технолгий.

Информация, содержащаяся в указанном письме может быть применены для проведения информационно-просветительсткой работы в трудовых коллективах и создания информационного контента.

Приложение на 2 л. в 1 л.

Председатель Комитета С. В. Портье

Комитет по делам образования города Челябинска
Документ подписан Электронной подписью
Сведения о сертификате ЭП
Кому выдан: Портье Светлане Викторовне
Серийный номер: 00 d5 e9 23 78 ff b9 ae 83
Срок действия: 16.05.2022 - 15.05.2027

М. А. Кинёва
700 18 70
Рассылка: МКУ «ЦОДОО», СП МКУ «ЦОДОО», ЦРО для рассылки во все ОУ

МВД России

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

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

04.10.2023 № 1/14157

на № _____ от _____

И.о. Министра образования и науки
Челябинской области

Е.А. Коузовой

О направлении информации

Уважаемая Елена Александровна!

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

1. Электронные письма на почту, которые приходят от «центра обмена сообщениями хостинга веб-почты», то есть от несуществующей организации. Авторы рассылки сообщают, что обновляют базу и удаляют все неиспользуемые учетные записи. Они настоятельно рекомендуют подтвердить электронную почту и обновить данные — так они будут знать, что аккаунт активен, и не будут его удалять. При этом не используются вредоносные программы и фишинговые сайты, необходимую мошенникам информацию (имя, фамилию, логин и пароль) просят прислать ответным сообщением. Таким образом мошенники получают доступ к личным данным граждан.

2. Мошенники стали чаще подделывать банковские приложения, например «Сбер 2.0» и «Поддержка Сбербанка». Злоумышленники звонят клиентам от имени сотрудника «Сбера» и убеждают установить приложения «Сбер 2.0» или «Поддержка Сбербанка». На самом деле под видом этих приложений киберпреступники распространяют программы для удаленного доступа к устройствам. Если пользователь установит одно из таких псевдоприложений, мошенники похищают его личную информацию и деньги с банковских карт.

3. Злоумышленники, маскируясь под представителя оператора связи, убеждают потенциальную жертву, что срок действия sim-карты истек. Для продления ее работы необходимо сообщить код из сообщения. После этого преступники подключают переадресацию звонков и SMS на другой номер и получают доступ к онлайн-банку, социальным сетям и мессенджерам жертвы для входа по номеру телефона.

4. Новые функции в телеграм-каналах – возможность публиковать сторис. Для этого необходимо получить определенное количество голосов «бустов» (голосов). В связи с этим появились чат-боты, предлагающие купить «бусты» в

больших количествах. Вводить данные банковской карты при этом не надо – просят выслать деньги обычным переводом. Пользователь переводит деньги, но по сути, не получает никаких гарантий, при этом у бота нет формы обратной связи.

5. Установка мобильного приложения с целью проверки качества работы смартфона. Фиктивная служба поддержки банка присылает ссылку на фишинговый сайт и предлагает подключить услугу безопасности смартфона. После того, как клиент соглашается на подключение и устанавливает на устройство мобильное приложение, мошенники получают доступ к онлайн-банку и похищают денежные средства.

6. Злоумышленники звонят от имени руководства компаний, организаций. Представляясь генеральным директором, мошенники предупреждают служащих, что им скоро поступит телефонный звонок от представителя курирующего эти компании Министерства. При этом, в мессенджерах используются аккаунты с реальными фотографиями и ФИО руководителей компаний, организаций. Далее действительно поступает звонок, в ходе разговора мошенники под различным предлогом получают конфиденциальную информацию, с целью совершения мошеннических действий.

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

С уважением,
Заместитель начальника –
начальник полиции И.В. Белецкий

исп. С.Н. Соколов
тел. 8 (351)267-72-60