

Самые популярные схемы мошенничества.

Выпускники школ – в центре внимания

Продажа «ответов» на задания ЕГЭ. Получив деньги, мошенники отправляют варианты прошлых лет или просто перестают отвечать жертве.

Аферисты создают фейковые сайты и группы в соцсетях, выдающие себя за приемные комиссии высших учебных заведений. Абитуриентам предлагают купить якобы бюджетные места, после получения денег злоумышленники пропадают.

Сообщения от неизвестных в мессенджере о том, что камера видеонаблюдения якобы зафиксировала списывание на ЕГЭ. Выпускнику предлагают выкупить запись. После перечисления средств связь обрывается, аккаунт мошенника блокируется.

аш отпуск под угрозой...

Злоумышленники предлагают липовые туры, бронирование билетов и жилья якобы по выгодным ценам.

Всегда внимательно проверяйте правильность написания названия сайта и пользуйтесь услугами проверенных компаний.

Концерта нет, а билеты есть!

Мошенники создают фишинговые сайты с афишей несуществующего выступления и заманивают туда потенциальных жертв.

Также фиксируется рост числа фишинговых сайтов, на которых аферисты предлагают заказать букеты, конфеты, парфюм и другие подарки якобы по оптовым ценам или с большими скидками.

«Моя племянница участвует в конкурсе...»

Одним из самых распространённых способов по угону аккаунтов в соцсетях и мессенджерах стали сообщения с просьбой проголосовать за ребенка, который участвует в каком-то конкурсе, а на кону – ценный приз.

Такие сообщения обычно приходят от кого-то из списка ваших контактов, чьей учетной записи уже получили доступ аферисты.

Переходя по ссылке для «голосования», вы попадаете на фишинговый сайт. Чтобы отдать свой голос, вас попросят авторизоваться. Если вы введете данные для входа в профиль, их получают злоумышленники.

Действие вашей SIM-карты истекает?

Телефонные мошенники обзванивают россиян под видом сотовых операторов с предложением продлить якобы истекающий договор на номер телефона.

В ходе разговора абоненту приходит сообщение с кодом, который необходимо ввести для «подтверждения пользовательского соглашения о продлении договора на новый срок».

Этот код – данные для входа в личный кабинет жертвы на портале «Госуслуги» или на других сервисах.

В действительности договоры, заключаемые абонентом с сотовыми операторами, бессрочные!

Ваш голос могут украсть

Злоумышленники активно используют нейросети. С их помощью они могут прислать голосовое и даже видеосообщение от имени вашего друга, которого взломали.

Также будьте внимательны с предложением о платной озвучке рекламы и фильмов, которую распространяют злоумышленники в сети. Собранные экземпляры голосов аферисты используют для обучения нейросетей и генерируют на их основе аудиосообщения, с помощью которых потом вымогают деньги у друзей и родственников жертвы.

На связи ваш «начальник»

Злоумышленники звонят и пишут в мессенджере пользователям под видом их начальников с работы. Для этого они создают реалистичные профили руководителей. Аферист сообщает жертве о каких-то проблемах и о том, что с ним свяжется «сотрудник» правоохранительных органов.

Второй мошенник в разговоре убеждает гражданина разными способами в том, что его деньги хотят украсть, перевести на счета СБУ или оформить на его имя кредит.

Вариаций много, но «спасительный ход» один – вывести деньги на «безопасный счет».

Фейковые электронные письма от госведомств

Пользователи получают электронные письма якобы от ФНС России, Роскомнадзора и других ведомств, в которых обычно говорится о каком-то

«нарушении» со стороны жертвы или иной «проблеме». С помощью такой рассылки аферисты заманивают россиян на фишинговые сайты, собирают персональные данные или распространяют зараженные вирусами файлы.

[#МВД](#) [#МВД74](#) [#Полиция74](#) [#Челябинскаяобласть](#) [#МВДРоссии](#) [#ПолицияК](#)
[атавИвановск](#) [#НеДайСебяОбмануть](#) [#Будьтебдительны](#)

