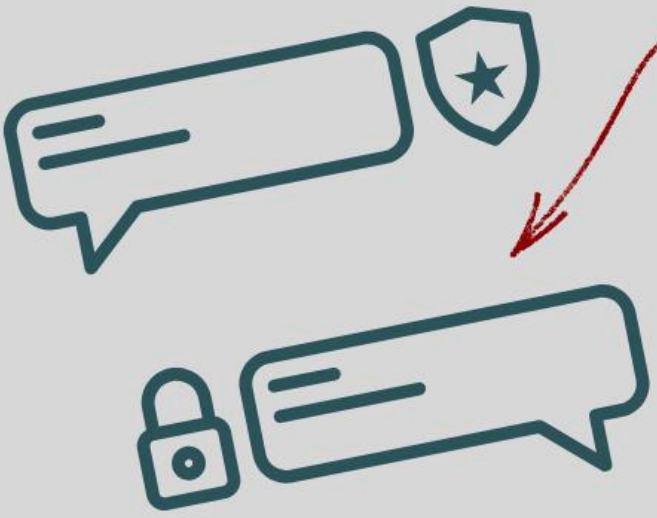
НИЦМП

Популярные схемы обмана 2.0

ЛОВУШКИ КИБЕРМОШЕННИКОВ



и как от них защититься

vk.com/nicmp

НИЦМП

Что нужно знать о мошенниках?

- Злоумышленники все чаще используют поддельные звонки «от банков», фейковые сообщения от госслужб и знакомых, а также фишинговые сайты, практически неотличимые от настоящих. Схемы мошенничества обновляются постоянно.
- Основной упор делается на срочность и страх, чтобы человек действовал быстро и не успел проверить информацию.
- Важно следить за «трендами» в сфере мошенничества, а также критически относиться к любым звонкам, сообщениям и просьбам.

Схемы здесь

vk.com/nicmp

КУРЬЕРСКАЯ ДОСТАВКА ИЗ МАРКЕТПЛЕЙСА

НИЦМП

Ф.И.О.
адрес

Вам звонят под видом маркетплейса и предлагают получить свой заказ курьерской доставкой.

Для убедительности называют ваши персональные данные.

Для подтверждения способа доставки просят назвать код из СМС или пуш-уведомления.

На самом деле вам поступает код для входа в банковское приложение или Госуслуги.

КАК ЗАЩИТИТЬСЯ

Не передавайте данные из СМС по телефону.

Маркетплейсы не запрашивают коды и другие личные данные по телефону.

ОШИБОЧНЫЙ ПЕРЕВОД

НИЦМП

На ваш счет поступают деньги, а затем сообщение об ошибочном переводе денег с прикрепленным pdf-файлом и просьбой возврата.

При отказе или сомнениях Вам угрожают судом.

После совершения обратного перевода вам начинают поступать угрозы о незаконном финансировании преступников.

Прикрепленный pdf-файл – фишинговый, мошенники получат доступ к вашим данным.

КАК ЗАЩИТИТЬСЯ

Свяжитесь с банком и оформите заявку на возврат ошибочно полученных средств.

Не открывайте pdf-файл и не пользуйтесь картой до списания средств, чтобы избежать обвинений в неосновательном обогащении.

ФЕЙКОВЫЕ ВЫПЛАТЫ

НИЦМП

Вам приходит СМС от «Госулуг» с обещанием выплаты, положенной по закону.

В письме есть ссылка, по которой нужно перейти, чтобы оформить ту самую выплату.

Открывается сайт, на котором вам необходимо оформить подписки на различные ресурсы (онлайн-казино, вредоносные приложения и тд.).

КАК ЗАЩИТИТЬСЯ

Зайдите на официальный сайт Госуслуг, проверьте информацию о выплатах в официальных СМИ.

Установите антивирусное ПО на всех гаджетах.

vk.com/nicmp

ЗВОНОК ИЗ НАЛОГОВОЙ

НИЦМП

Вам звонят от имени Федеральной налоговой службы и говорят о том, что работодатель не предоставил справку о доходах сотрудников и угрожают штрафами.

Вас убеждают, что помогут направить запрос работадателю и записать на прием, а для подтверждения записи нужно назвать код из СМС.

Код подтверждает изменение пароля от Госулуг и мошенники входят в ваш аккаунт.

КАК ЗАЩИТИТЬСЯ

Сотрудники ФНС не связываются по телефону для записи на прием и не запрашивают личные данные.

Информацию проверяйте только на официальном сервисе ФНС России.

Обратитесь в правоохранительные органы.

ТЕХНИКА С БОЛЬШОЙ СКИДКОЙ

НИЦМП

Вы натыкаетесь на телеграмм-канал о продаже техники с выгодой до 60%, с большим количеством подписчиков и реакций на постах.

После внесения оплаты, вы получаете заверения, что техника отправлена. Но посылку якобы задерживают на границе, а чтобы она поехала дальше, необходимо доплатить.

После доплаты собеседник вносит вас в черный список либо удаляет аккаунт.

КАК ЗАЩИТИТЬСЯ

Свяжитесь с банком и оформите заявку на блокировку перевода.

Сделайте скриншоты переписки и деталей платежа и обратитесь в правоохранительные органы.

НЕСОСТОЯВШАЯСЯ ФОТОСЕССИЯ

НИЦМП

Фотограф предлагает бесплатную фотосессию. Необходимо забронировать и оплатить студию, которую предлагает сам фотограф.

Перед мероприятием фотограф сообщает об отмене, и вам необходимо сделать возврат оплаты в студии.

Ссылка, отправленная студией, приводит на оформление возврата. После ввода номера карты деньги не возвращаются, а еще раз списываются.

КАК ЗАЩИТИТЬСЯ

- Найдите работы фотографа через опцию «Поиск по фото», чтобы убедиться в подлинности.
- Проверьте студию по поиску в интернете, адресу, отзывам, сверьте контакты для связи.
- Обратитесь в банк и правоохранительные органы.

ЧТО СТОИТ ЗАПОМНИТЬ

НИЦМП

НИКОМУ И НИКОГДА НЕ СООБЩАЙТЕ КОДЫ ИЗ SMS, PUSH-УВЕДОМЛЕНИЙ И ПРИЛОЖЕНИЙ

Ни «сотрудникам банка», ни «службе безопасности», ни «знакомым». Настоящие компании никогда не спрашивают такие коды.

ПРОВЕРЯЙТЕ ОТПРАВИТЕЛЯ, А НЕ ТЕКСТ

Подделать можно логотипы, стиль речи. Всегда смотрите на адрес отправителя, домен сайта, номер телефона. Даже одна лишняя буква — признак фейка.

НЕ ПЕРЕХОДИТЕ ПО ССЫЛКАМ ИЗ SMS

Даже если сообщение выглядит официально. Заходите на сайты и в приложения только вручную или через закладки.

ЧТО СТОИТ ЗАПОМНИТЬ

НИЦМП

НЕ ВВОДИТЕ ДАННЫЕ КАРТЫ И ПАРОЛИ НИГДЕ, КРОМЕ ОФИЦИАЛЬНЫХ СЕРВИСОВ

CVV, PIN, логины и пароли — это секрет. Потеря этих данных = потеря денег и аккаунтов.

НЕ ДОВЕРЯЙТЕ СООБЩЕНИЯМ О СРОЧНОСТИ

Если сообщение требует немедленных действий — это почти всегда обман. Остановитесь и перепроверьте информацию через официальный сайт или приложение.

ВКЛЮЧАЙТЕ ДВУХФАКТОРНУЮ АУТЕНТИФИКАЦИЮ

Даже если пароль украдут, второй фактор (приложение или ключ) защитит аккаунт.