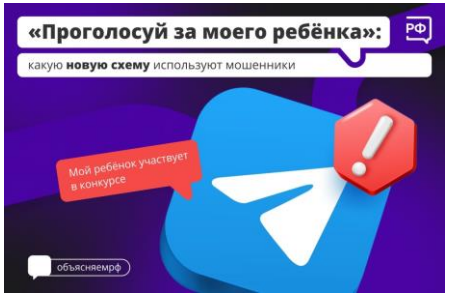

«Мой ребёнок участвует в конкурсе, проголосуй за его рисунок», — пишут мошенники в «Телеграме» от имени вашего знакомого.

Аферисты взламывают аккаунт человека, а затем пишут всем из списка контактов с просьбой проголосовать в конкурсе — например, за его ребёнка. К сообщению преступники прикрепляют фишинговую ссылку: если по ней перейти и ввести свои данные, мошенники получат доступ к вашему телеграм-аккаунту.

Как защититься:

- не переходите по незнакомым и подозрительным ссылкам;
- если ссылка ведёт на знакомый вам сайт, проверьте её — она должна начинаться с https, без лишних или заменённых символов: мошенники часто делают ссылки похожими на настоящие, но добавляют либо меняют в них несколько букв или знаков, например l вместо;
- позвоните человеку, который вам написал, чтобы удостовериться, действительно ли он отправил это сообщение;
- если вы всё же перешли по ссылке, найдите значок замка в начале адресной строки — он означает безопасное соединение;
- чтобы максимально обезопасить свой аккаунт, используйте двухфакторную аутентификацию — тогда, если мошенники попытаются войти в ваш профиль, им потребуется не только пароль, но и код из СМС.

У вас тут
это…НЕЛЕГАЛЬНАЯ ЗАНЯТОСТЬ!

В Краснодарском крае участились случаи мошеннических действий в отношении органов исполнительной власти и работодателей.

Схема выглядит следующим образом: злоумышленники рассылают уведомления о выявленных признаках нелегальной занятости, выдавая себя за межведомственную комиссию. В этих сообщениях предлагают оплатить государственную пошлину через QR-код

Обращаем ваше внимание!

Межведомственная комиссия по противодействию нелегальной занятости в Краснодарском крае, а также муниципальные рабочие группы НЕ ТРЕБУЮТ от работодателей оплаты государственной пошлины

Не переходите по ссылкам, и не осуществляйте платежи

Гибкий график, стабильный доход, удалённая работа, например копирайтером или контент-менеджером, — мошенники публикуют заманчивые вакансии, чтобы получить доступ к вашим банковским счетам.

Под видом работодателей они публикуют в мессенджерах объявления о поиске сотрудников, которых якобы готовы взять без опыта и обучить за счёт компании.

Затем они просят установить специальное приложение для работы. На самом деле это вирус-шпион, который будет перехватывать ваши СМС. С его помощью злоумышленники получат коды для входа в ваши аккаунты и подтверждения банковских операций.

Как защититься:

- ищите работу на проверенных площадках для найма и сайтах компаний-работодателей;
- вас должно насторожить, если зарплата, которую обещают, гораздо выше, чем на аналогичных должностях в других компаниях, или если вас торопят с принятием решения;
- не устанавливайте приложения по просьбе «работодателей» и не переходите по подозрительным ссылкам от них.

Фишинговые ссылки на «подарки»

Мошенники начали массово рассылать сообщения с предложением отследить «подарок» по ссылке, ведущей на фишинговый сайт. Жертву просят оплатить доставку, ввести персданные или подтвердить личность. На таких сайтах злоумышленники могут установить вредоносное ПО, списать деньги или украсть данные банковских карт. *Эксперты советуют насторожиться, если вы получили сообщение о неожиданном подарке, особенно с незнакомого адреса или с подозрительными требованиями.*

«Коробочный» скам

Схема предполагает участие в якобы розыгрыше ценных призов, таких как техника, деньги или автомобили. На поддельных сайтах участникам предлагают «открывать коробки» с призами, но для получения выигрыша нужно оплатить доставку или налоги. В результате деньги уходят мошенникам, а данные банковских карт становятся компрометированными. *Будьте внимательны: проверяйте информацию о розыгрышах и не переходите по подозрительным ссылкам.*

Фейковые «Госуслуги»

Злоумышленники создают поддельные сайты, маскирующиеся под справочные порталы «Госуслуг», и публикуют на них фальшивые номера поддержки. Пользователи, поверившие в их достоверность, звонят на эти номера, где мошенники под видом операторов выманивают данные для входа в аккаунты. Чтобы не стать жертвой, *проверяйте номера телефонов на официальном сайте и игнорируйте сообщения о «взломе», которые содержат сомнительные контакты.*

Как себя защитить?

- Не переходите по сомнительным ссылкам, даже если сообщение кажется правдоподобным, и не вводите личные данные на незнакомых сайтах.
- Убедитесь, что вы используете только официальные номера телефонов для связи с важными сервисами, такими как «Госуслуги».
- При подключении к интернету избегайте использования VPN-сервисов, особенно бесплатных, которые могут не только не защитить ваши данные, но и стать инструментом в руках злоумышленников.

Сайты:
https://vk.com/kcson_slavyansk23

http://slavyanskij-kcson.ru.

МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОГО РАЗВИТИЯ КРАСНОДАРСКОГО КРАЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ КРАСНОДАРСКОГО КРАЯ «СЛАВЯНСКИЙ КОМПЛЕКСНЫЙ ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ»

Отделение развития инновационных форм социального обслуживания

КАК ЗАЩИТИТЬ СЕБЯ ОТ МОШЕННИКОВ

г. Славянск-на-Кубани