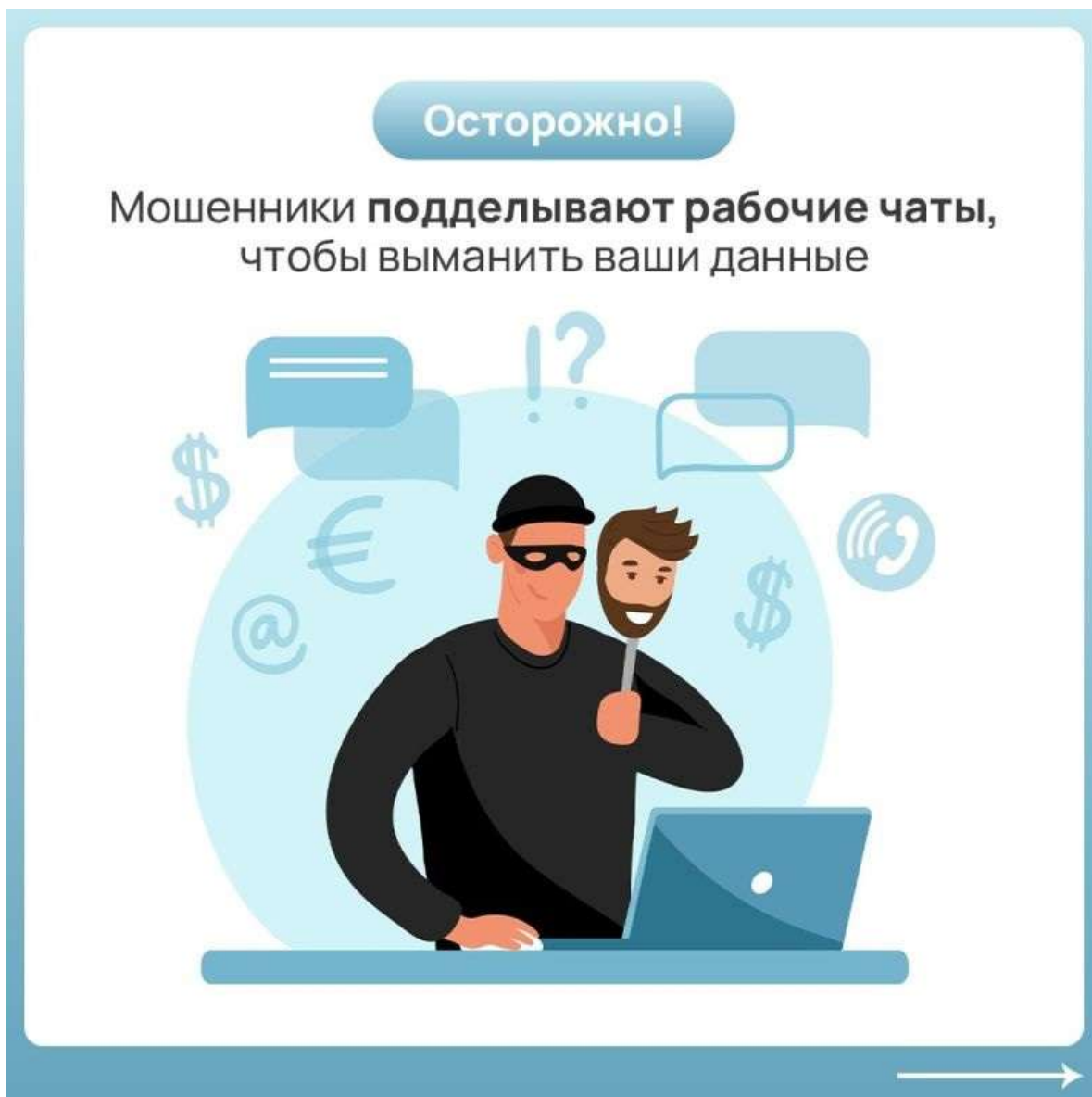


Один из видов мошенничества - новые рабочие чаты



Мошенники имитируют рабочий чат с вашими коллегами, получая обманным путем доступ к персональным и учетным данным.

Как работает:

Вам приходит приглашение в новый чат с наименованием вашей компании или подразделения. В этом чате заранее созданы поддельные аккаунты ваших коллег и руководителей. С аккаунтов «ваших руководителей» мошенники будут отправлять сообщения и ставить рабочие задачи, например, о необходимости передать персональные и учетные данные якобы в «отдел кадров». Другие поддельные аккаунты будут подтверждать важность задачи и отчитываться о выполненной работе.

Что требуют:

Заполнить форму с персональными данными, предоставить коды авторизации для госуслуг.

Как защититься:

- Проверяйте любые новые контакты в общедоступных мессенджерах другим путем, спрашивайте ваших коллег, самостоятельно звоните им по телефону, напишите по электронной почте.
- Не доверяйте ссылкам, файлам и формам на внешних сайтах.
- Не передавайте коды авторизации из СМС и пуш-сообщений.

Соблюдайте общие правила цифровой гигиены:

1. Никому не сообщайте коды из SMS.
2. Не переходите по подозрительным ссылкам. Вводите адреса сайтов вручную.
3. Не устанавливайте непонятные приложения по просьбе незнакомых людей.
4. Не поддавайтесь на давление. Срочность – главное оружие мошенников.
5. Проверяйте информацию. Позвоните в официальную службу поддержки вашего банка или госоргана.

Бдительность и здоровый скептицизм – ваша лучшая защита в цифровом мире. Помните: если предложение кажется слишком выгодным или проблема требует немедленных денежных переводов – это почти наверняка ловушка.

Разъяснение подготовлено прокурором Клинцовского района В. И. Родиным