



ПРОКУРАТУРА
Российской Федерации

ПРОКУРАТУРА
Иркутской области
Прокуратура
Куйтунского района
ул.Карла Маркса,17 «а»
п.Куйтун, 665302



Мэру муниципального образования
«Куйтунский район»
Непомнящих А.А.

Главе Куйтунского городского
поселения

Яковлевой Л.И.

Главам Андрюшинского, Алкинского,
Барлукского, Большекашелаковского,
Иркутского, Каразейского, Карымского,
Куйдунского, Ленинского,
Лермонтовского, Мингатуйского,
Новотельбинского, Панагинского,
Тулушского, Усть-Кадинского,
Уховского, Уянского, Харикского,
Чеботарихинского сельских поселений

16.04.2025 № 11-13-2025/716-25-20250029

штамп регистрации

В соответствии с п. 3.5. Инструкции о порядке рассмотрения обращений и В соответствии с п.п. 1.2 – 1.4 Приказа Генпрокуратуры России от 02.08.2018 № 471 «Об организации в органах прокуратуры Российской Федерации работы по правовому просвещению и правовому информированию» направляем в Ваш адрес информацию разъяснительного характера на тему «Мошенническая схема с обновлением банковских приложений» для опубликования на сайте администрации муниципального образования, в группах с использованием мессенджера «Viber», «Watsap», «Telegramm».

Приложение: информация на 1 л.

И.о. прокурора района

советник юстиции

В.З. Галеев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 677D3D35B61360A221690F4E35F65755
Владелец Галеев Василий Зифарович
Действителен с 15.03.2024 по 08.06.2025

Н.С. Виноградова 038-390-629

Прокуратура Куйтунского района Иркутской
области

№ 11-13-2025/716-25-20250029

Прокуратура Куйтунского района разъясняет Мошенническая схема с обновлением банковских приложений.

Мошенники начали чаще похищать деньги, представляясь сотрудниками банка и призывая срочно обновить мобильное приложение.

Злоумышленники звонят и представляются сотрудниками банка, убеждая установить «правильную версию» приложения. Они настаивают на немедленном обновлении, иначе счета и карты клиента могут быть заблокированы.

Затем мошенники присылают ссылку для скачивания обновления, которая ведет на специальный ресурс. После перехода экран блокируется, давая злоумышленникам доступ к устройству, в том числе в личный кабинет банковского приложения. Мошенники используют перехваченные смс-коды для вывода денежных средств со счета жертвы.

Не переходите по сомнительным ссылкам: скачивайте и обновляйте приложения только через официальные приложения.

Не доверяйте неожиданным звонкам: банки не просят обновлять приложение по телефону или через мессенджеры.

Свяжитесь с банком самостоятельно: при любых сомнениях позвоните в банк по официальному номеру, указанному на вашей карте или на официальном сайте банка.

Блокируйте доступ при подозрениях: если вы уже перешли по подозрительной ссылке, немедленно обратитесь в банк и попросите временно заблокировать личный кабинет.

Берегите свои финансы и будьте бдительны к подобным попыткам обмана!