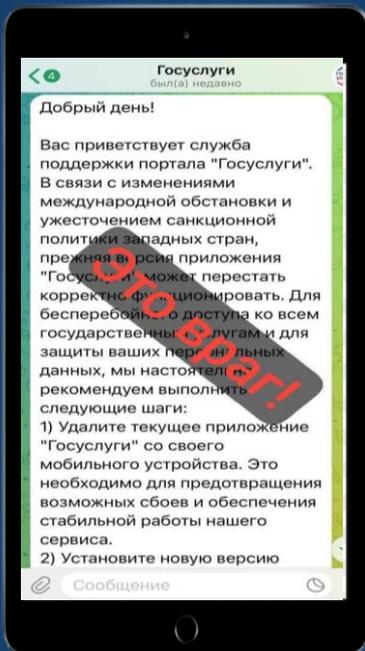
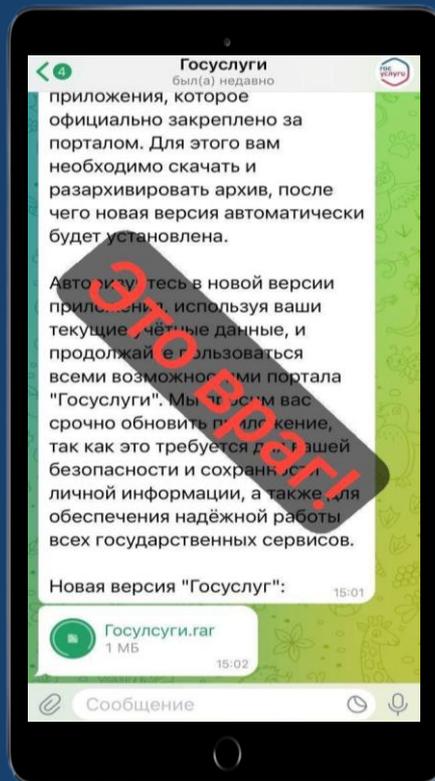


**Прокуратура
г.Бодайбо
информирует:
«НЕ поддавайтесь
уловкам
МОШЕННИКОВ!!»**



⚠ Под предлогом «обновления» приложения Госуслуги преступники рассылают загрузочные файлы в мессенджере от имени Единого государственного портала.



Госуслуги никогда не станут рассылать подобные сообщения.

⊖ Не верьте подобным провокациям. Не скачивайте файлы и заблокируйте собеседника.

⚠ **Фальшивые
квитанции в
почтовом
ящике!**

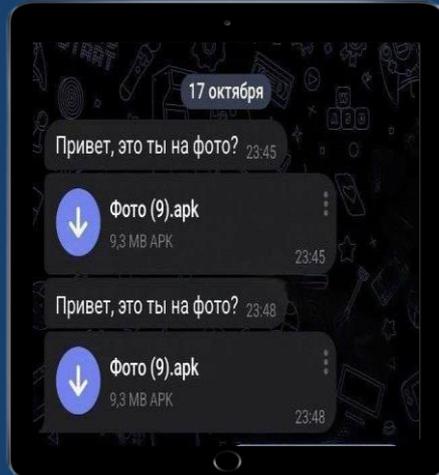


Мошенники раскладывают поддельные долговые платежные документы в почтовые ящики жильцов многоквартирных домов. Отсканировав QR-код жертва переходит по фишинговой ссылке. При оплате несуществующей задолженности деньги перечисляются на счет злоумышленников.

Ⓜ Кроме того, аферисты могут получить доступ к вашим персональным данным и электронным сервисам: госуслуги, онлайн-банкинг. Во избежание неприятностей перепроверяйте документы с ранее поступившими квитанциями!



Хищение телеграм аккаунтов



Обман в мессенджерах с помощью поддельных профилей популярных сервисов доставки



Мошенники выдают себя за службу поддержки мессенджера. Затем сообщают жертве о якобы поданной заявке на удаление аккаунта. После этого аферисты просят назвать код из СМС и перенаправляют на фейковый сайт, что приводит к потере контроля над профилем.

Ни в коем случае не загружайте «фотографии» с расширением APK



Важно
Фотофайлы не могут иметь формат APK. Данное расширение используется для установки приложений

Злоумышленники маскируют фишинговые приложения под фотографии. После загрузки файла на устройство устанавливается вредоносное ПО для хищения персональных данных или денежных средств.



От имени псевдоофициального аккаунта мошенники присылают сообщения о том, что заказ якобы готов к выдаче. Чтобы узнать подробности или отследить посылку предлагают перейти на сайт, где пользователю нужно ввести номер карты, имя и пароль от онлайн-банка. Так лжедоставщики получают доступ к деньгам своих жертв.



⚠️ Фальшивые квитанции в почтовом ящике! ⚠️



Мошенники раскладывают поддельные долговые платежные документы в почтовые ящики жильцов многоквартирных домов. Отсканировав QR-код жертва переходит по фишинговой ссылке. При оплате несуществующей задолженности деньги перечисляются на счет злоумышленников. Кроме того, аферисты могут получить доступ к вашим персональным данным и электронным сервисам: госуслуги, онлайн-банкинг. Во избежание неприятностей перепроверяйте документы с ранее поступившими квитанциями!



⚠️ Под предлогом «обновления» приложения Госуслуги преступники рассылают загрузочные файлы в мессенджере от имени Единого государственного портала.

⊖ Не верьте подобным провокациям. Не скачивайте файлы и заблокируйте собеседника.

Прокуратура г.Бодайбо информирует: «НЕ поддавайтесь уловкам МОШЕННИКОВ!!»



Госуслуги никогда не станут рассылать подобные сообщения.

