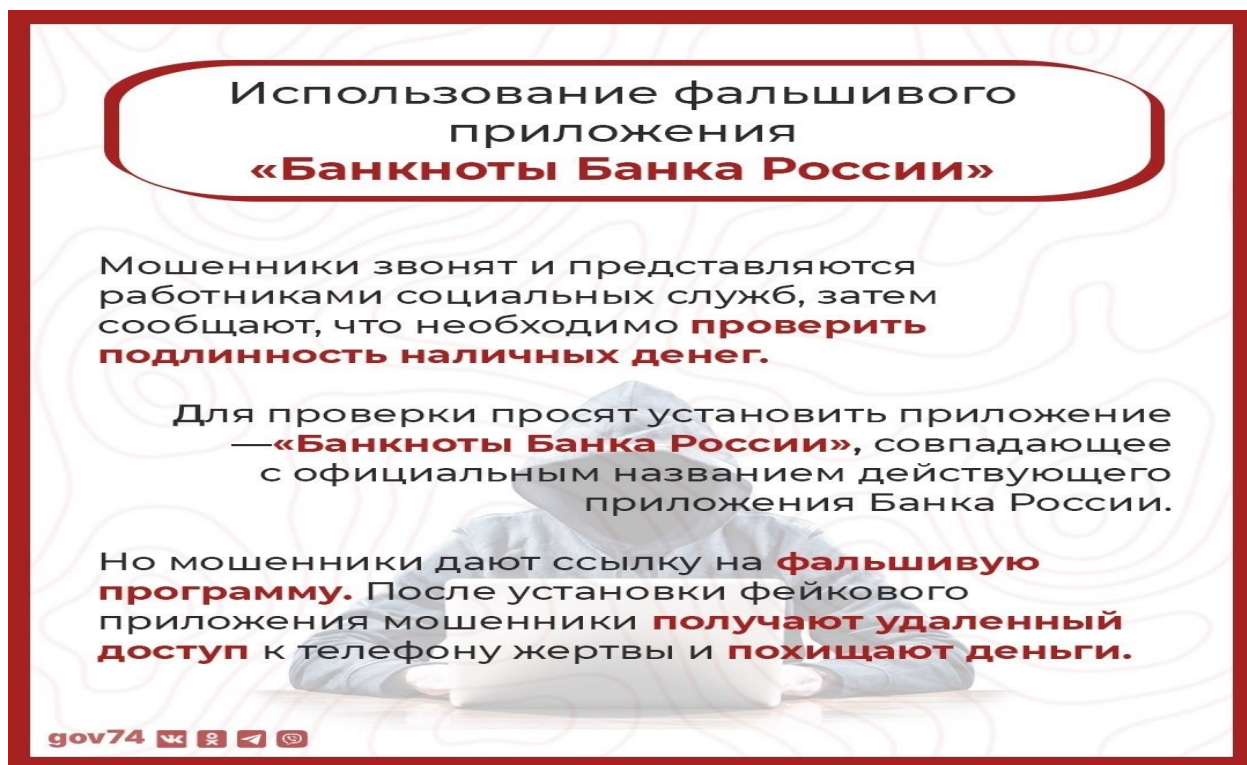
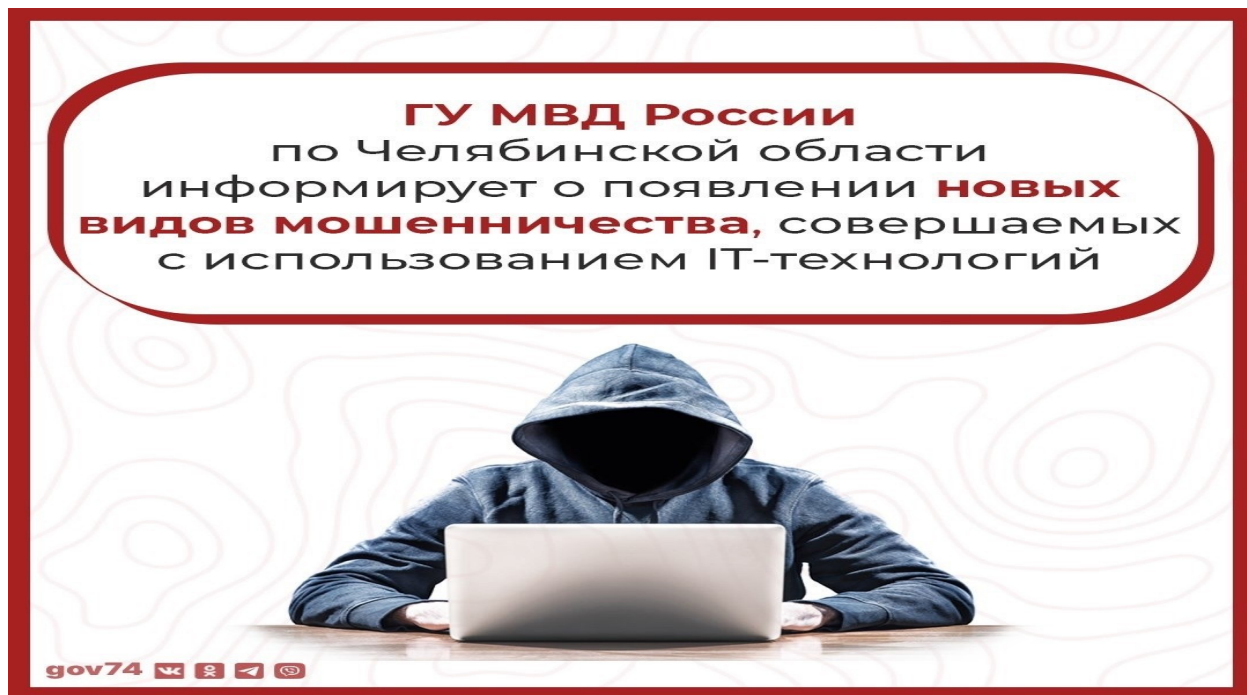


Схемы IT-мошенничества продолжают совершенствоваться. Чтобы не попасться на их уловки, ознакомьтесь с карточками, подготовленными УОС Правительства Челябинской области.

[#МВДРоссии](#) [#МВД74](#) [#Полиция74](#) [#Челябинскаяобласть](#) [#ПолицияЮжного Урала](#) [#ПолицияКатавИвановскийрайон](#) [#Мошенничество](#) [#Профилактика](#)



Мошенничество по схеме «Демонстрация экрана смартфона»

На телефоны граждан поступают звонки **от якобы сотрудника банка**, с предложениями **дополнительного заработка, оформления кредита.**

Далее мошенники настаивают продолжить **разговор только по видеосвязи**, затем **просят включить демонстрацию экрана** смартфона, чтобы увидеть уведомления на смартфоне.

Это позволяет злоумышленникам **изменить старый пароль входа в онлайн-банк** и установить новый.

Затем мошенники **получают доступ** к мобильному банку и **похищают денежные средства.**

gov74



Мошенничество под предлогом оплаты товара по **QR-коду**, через «систему быстрых платежей»

Покупатель, заинтересовавшись дорогостоящим товаром, **оставляет заявку на сайте**, который на самом деле является **поддельным.**

Затем, покупателю **поступает звонок якобы от продавца магазина** и предлагает приобрести **товар со скидкой** при условии оплаты через «систему быстрых платежей» по **QR-коду.**

В случае согласия, злоумышленник отправляет ссылку на **фишинговый сайт** с формой оплаты по QR-коду.

Как только **покупатель совершает платеж, деньги отправляются на счет мошенника.**

gov74

