# БУДЬТЕ БДИТЕЛЬНЫ!

В случае совершения в отношении Вас дистанционного мошенничества обращайтесь в дежурную часть МО МВД России «Ливенский»

**8 (48677) 7-20-75; 8 (48677) 7-03-84**

**Орловская область, г. Ливны, ул. Орджоникидзе, д. 4, 303850**

ЛИВЕНСКАЯ МЕЖРАЙОННАЯ ПРОКУРАТУРА ОРЛОВСКОЙ ОБЛАСТИ

## ПАМЯТКА

# «КАК НЕ СТАТЬ ЖЕРТВОЙ ДИСТАНЦИОННОГО МОШЕННИЧЕСТВА»

2024 год

## Для предотвращения противоправных действий по дистанционному хищению денежных средств необходимо следовать следующим **ПРАВИЛАМ:**

* Сотрудники правоохранительных органов, банковских учреждений и других органов никогда по телефону или в электронном письме не запрашивают:

- персональные сведения;
- реквизиты и срок действия банковской карты;
- пароли или коды из СМС-сообщений для подтверждения финансовых операций или их отмены;
- логин, ПИН-код и CVV-код банковских карт.

* Сотрудники правоохранительных органов, банковских учреждений и других органов не предлагают:

- установить программы удаленного доступа (или сторонние приложения) на мобильное устройство и разрешить подключение к ним под предлогом технической поддержки (например, удаление вирусов с устройства);
- перейти по ссылке из СМС-сообщения; включить переадресацию на телефоне клиента для совершения в дальнейшем звонка от его имени в банк;
- под их руководством перевести для сохранности денежные средства на «защищённый счёт»;
- зайти в онлайн-кабинет по ссылке из СМС-сообщения или электронного письма.

* Необходимо учитывать, что держатель карты обязан самостоятельно обеспечить конфиденциальность ее реквизитов и в этой связи избегать:

- подключения к общедоступным сетям Wi-Fi;
- использования ПИН-кода или CVV-кода при заказе товаров и услуг через сеть «Интернет», а также по телефону;
- сообщения кодов третьим лицам (в противном случае любые операции, совершенные с использованием ПИН-кода или CVV-кода, считаются выполненными самим держателем карты и не могут быть опротестованы).

* При использовании банкоматов необходимо отдавать предпочтение тем, которые установлены в защищённых местах (например, в госучреждениях, офисах банков, крупных торговых центрах).

* При использовании мобильного телефона необходимо соблюдать следующие правила:

- при установке приложений быть осторожным, если запрашиваются права на чтение адресной книги, отправку СМС-сообщений и доступ к сети «Интернет»;
- применяя сервисы СМС-банка, необходимо сверять реквизиты операции в СМС-сообщении с одноразовым паролем от официального номера банка. Если реквизиты не совпадают, то такой пароль вводить нельзя.

* В случае смены номера мобильного телефона или его утери необходимо связаться с банком для отключения и блокировки доступа к СМС-банку и заблокировать сим-карту, обратившись к сотовому оператору.

* При оплате услуг картой в сети «Интернет» необходимо использовать только проверенные сайты, внимательно прочитывать тексты СМС-сообщений с кодами подтверждений, проверять реквизиты операции.