

 Фишинг - один из самых распространенных способов обмана в Интернете

Чтобы не стать жертвой, проверяйте информацию о сайте на специальных платформах.  
Одной из таких является: [www.reg.ru](http://www.reg.ru) ([www.reg.ru/](http://www.reg.ru/))

 После ввода адреса сайта там высветится информация о нем.

 Не дайте себя обмануть

[#полицияКатавИвановск](#) [#полиция74](#) [#МВД74](#) [#ОстановиМошенника](#)  
[#НеДайСебяОбмануть](#)

# Фишинговые письма

или как распознать  
**мошенника**



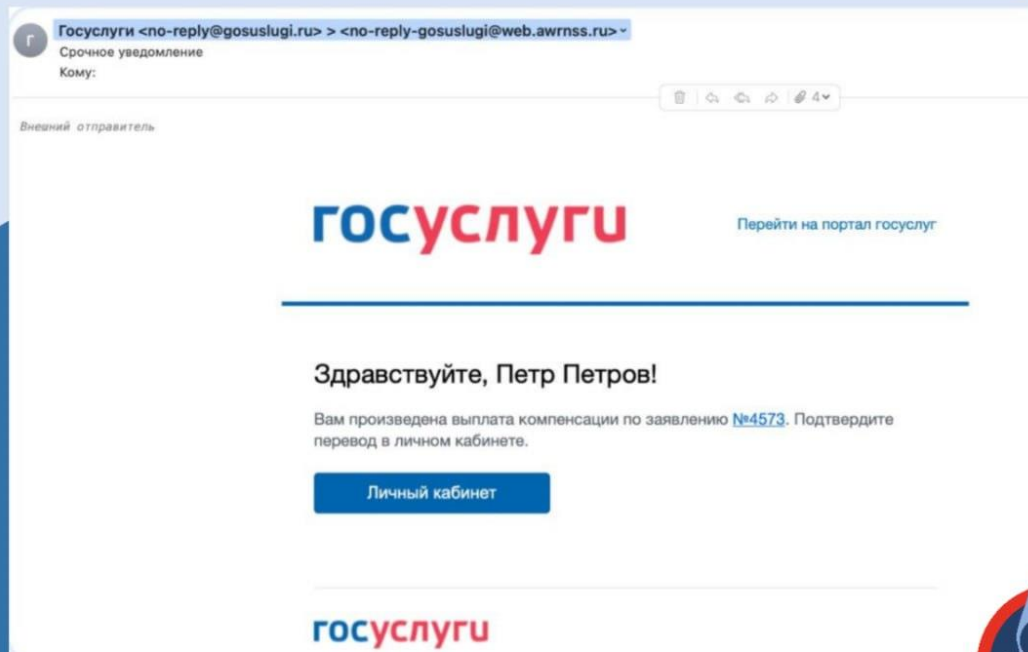
**Фишинговые сайты** создают для хищения личной информации пользователя. Даже очень осторожный человек может стать жертвой обмана.





Такой метод распространен в мессенджерах, соцсетях, смс и электронных письмах. **Самая популярная схема** — отправка сообщений со ссылкой на фишинговый сайт, где нужно ввести данные.

# Одна из фишинговых рассылок аферистов



Преступники обычно **подделывают** сайты:

- государственных сервисов (например, сайта «Госуслуги»);
- интернет-магазинов;
- служб такси и доставки;
- систем онлайн-оплаты;
- сервисов для операции с криптовалютой.



## Признаки фишингового сайта:

- Мошеннические сайты могут использовать доменные имена, похожие на настоящие, но содержащие опечатки или изменения;
- добавляются слова к известным доменным именам;
- фишинговые сайты применяют менее распространенные доменные зоны (например, .xyz, .top);
- наличие ошибок на онлайн-странице.



## Как себя обезопасить?

WHOIS — открытая база, в которой хранится информация о доменах, их владельцах, сроках регистрации и IP-адресах. Существует множество онлайн-сервисов, которые позволяют получить эту информацию.

[www.reg.ru](http://www.reg.ru)

