

Чтобы не стать жертвой фишинга в социальной сети или мессенджере, необходимо выполнять следующие рекомендации:

1. Если вы получили от вашего знакомого сообщение с просьбой перевести деньги или перейти по ссылке, свяжитесь с ним по другим каналам и уточните, действительно ли он вам об этом писал.
2. Будьте внимательны, когда открываете сообщения от неизвестных отправителей.
3. Не доверяйте сомнительным предложениям, не переходите по подозрительным ссылкам, особенно если они скрыты сервисом коротких URL.
4. Для проверки подозрительных URL-ссылок (особенно коротких) используйте бесплатные сервисы, например, VirusTotal.
5. Подключите двухфакторную аутентификацию для доступа к аккаунту, не сообщайте никому код авторизации.
6. Используйте уникальный пароль для каждого сервиса.
7. При малейшем подозрении на взлом аккаунта немедленно смените все пароли.
8. Установите на используемые устройства антивирусную программу и регулярно её обновляйте.
9. Не игнорируйте предупреждения браузера, если он сообщает о переходе на недоверенный ресурс или на сайт с некорректными сертификатами безопасности.

[#МВДРоссии](#) [#МВД](#) [#МВД74](#) [#Полиция74](#) [#Челябинскаяобласть](#) [#ПолицияЮжногоУрала](#) [#ПолицияКатавИвановскийрайон](#) [#Профилактика](#) [#Мошенничество](#)