# Не попадись на удочку фишинга!

Фишинг - это когда преступники пытаются вынудить вас сделать что-то для них полезное, например, поделиться учетными данными, перевести средства или открыть вложения электронной почты. Такие атаки часто начинаются с фишинга.

Не упустите эти десять контрольных признаков фишинговых писем и убедитесь, что вы не стали жертвой фишинга.

1. Письмо кажется неправильным. Полагайся на свое чутье.
2. Общие приветствия. Остерегайтесь безличных приветствий, таких как "Уважаемый покупатель."
3. Запрос конфиденциальных данных. Хакеры подделывают подлинные веб-сайты и пытаются обмануть вас при вводе личных данных.
4. Конкретная информация о вас. Мошенники используют информацию, найденную в интернете, чтобы выглядеть более убедительно.
5. Тактика запугивания. Запугивающие фразы часто используются, чтобы заставить вас действовать, не задумываясь.
6. Грамматические или орфографические ошибки. Сами себя выдают.
7. Срочность выполнения. Остерегайтесь вынужденного давления на время. Это обычная тактика.
8. "Вы выиграли главный приз!" Это распространенные фишинговые письма, их легко обнаружить.
9. "Подтвердите свой аккаунт." Всегда выясняйте причину подтверждения.
10. Киберквоттинг. Остерегайтесь похожих URL-адресов, предназначенных для обмана, например: www.g00gle.com or www.hotmai1.com.

Узнайте больше о фишинге и о том, как остановить его на sophos.com/prevent-phishing?id=00130000019KE2V

SOPHOS