Прокуратура Ленинского района
г. Севастополя

# ФИШИНГ

- хакерская атака, при которой персональные данные и деньги похищают с помощью фиктивных сайтов, аккаунтов или электронных писем.

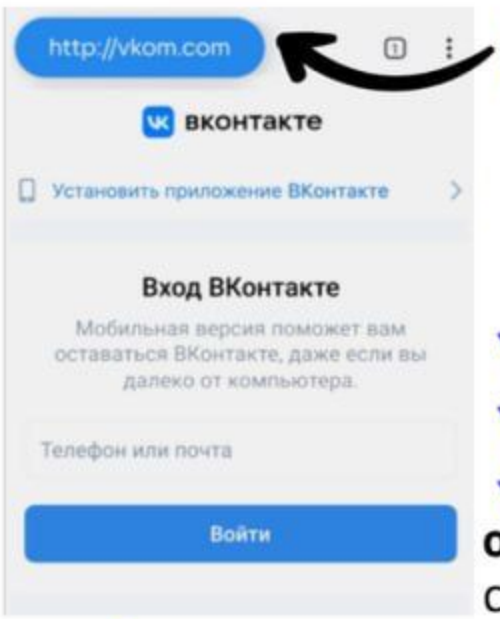
## ЧТО ТАКОЕ ФИШИНГОВАЯ АТАКА?

Фишинг проходит по **электронной почте, SMS, в мессенджерах** и в **социальных сетях.**



**Атака выглядит так:** человек **получает сообщение** от сервисов, которым доверяет. Например, от своего банка или маркеплейса, где недавно совершил покупку. **В этом письме его просят срочно указать личные данные или обновить их или сообщают о выигрыше бонусов за покупку, которые необходимо срочно активировать.**

Если приглядеться к такому письму или СМС, можно заметить, что ссылка **не совпадает с официальными контактами** сервиса, банка или магазина, именно она и ведет на копию официального сайта. **Если пользователь введёт там свои данные, то они попадут к мошенникам.**




Пример фишинговой ссылки

## КАК ЗАЩИТИТЬСЯ ОТ ФИШИНГОВЫХ АТАК?

✓ **Не отвечайте на подозрительные сообщения;**

✓ **Проверьте адрес отправителя;**

✓ **Используйте антивирусное программное обеспечение**, оно помогает защитить компьютер от спам-сообщений;

✓ **Будьте осторожны, совершая онлайн-покупки.** При покупке товаров или услуг убедитесь, что сайт использует безопасный протокол передачи данных, — **в строке с адресом сайта должно быть написано** https, а не http.