Памятка: фишинг и безопасные ссылки

Как распознавать подделки и не отдавать данные мошенникам.

Признаки фишинга

- Срочность: «срочно подтвердите», «аккаунт будет заблокирован».
- Необычный адрес отправителя или домен сайта (лишние буквы, дефисы).
- Просьба ввести пароль/код из смс/данные карты.
- Ошибки в тексте, странный дизайн, неработающие элементы сайта.

Как проверить ссылку

- Наведи курсор и посмотри, куда ведёт ссылка (на телефоне — удержание).
- Сравни домен с официальным (например, school.ru, gosuslugi.ru).
- Не вводи пароль по ссылке из письма — открой сайт вручную.

Тренировка

Отметьте, что безопаснее:

Ситуация	Безопасно	Опасно	Почему?
Письмо «Вы выиграли приз, войдите по ссылке»			
Сайт открылся, но адрес отличается на 1 букву			
Друг прислал ссылку «посмотри фото» без пояснений			
Вход в сервис через сохранённую закладку			

Совет: добавьте на уроке разбор примеров адресов (без перехода по подозрительным ссылкам).