

Пароль

- **Использовать длинные комбинации** — короткие пароли на 4–6 символов проще запомнить, но легче взломать.
- **Чередовать разные символы:** цифры с буквами в верхнем и нижнем регистре, специальные символы (!, @, #, \$, %).
- **Не использовать простые сочетания:** даты рождения, имена, клички животных, популярные слова или буквы, расположенные в ряд на клавиатуре.
- **Создавать разные пароли для разных аккаунтов** — если взломают одну учётную запись, остальные тоже будут под угрозой.

Переписка

- **Проверять отправителя** — не доверять только имени, всегда проверять полный адрес.
- **Не переходить по ссылкам** в письмах от неизвестных отправителей — они могут вести на фишинговые сайты.
- **Проверять письма, в которых содержатся призывы к действиям** (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы.

Вложения

- **Не открывать вложения**, если не уверены в надёжности отправителя. Например, не открывать документы с макросами, архивы с паролями, файлы с расширениями RTF, LNK, CHM, VHD.
- **Если письмо содержит поясняющий текст к вложению**, его необходимо также передать адресату вместе с вложением (распечатанным или в электронном виде).