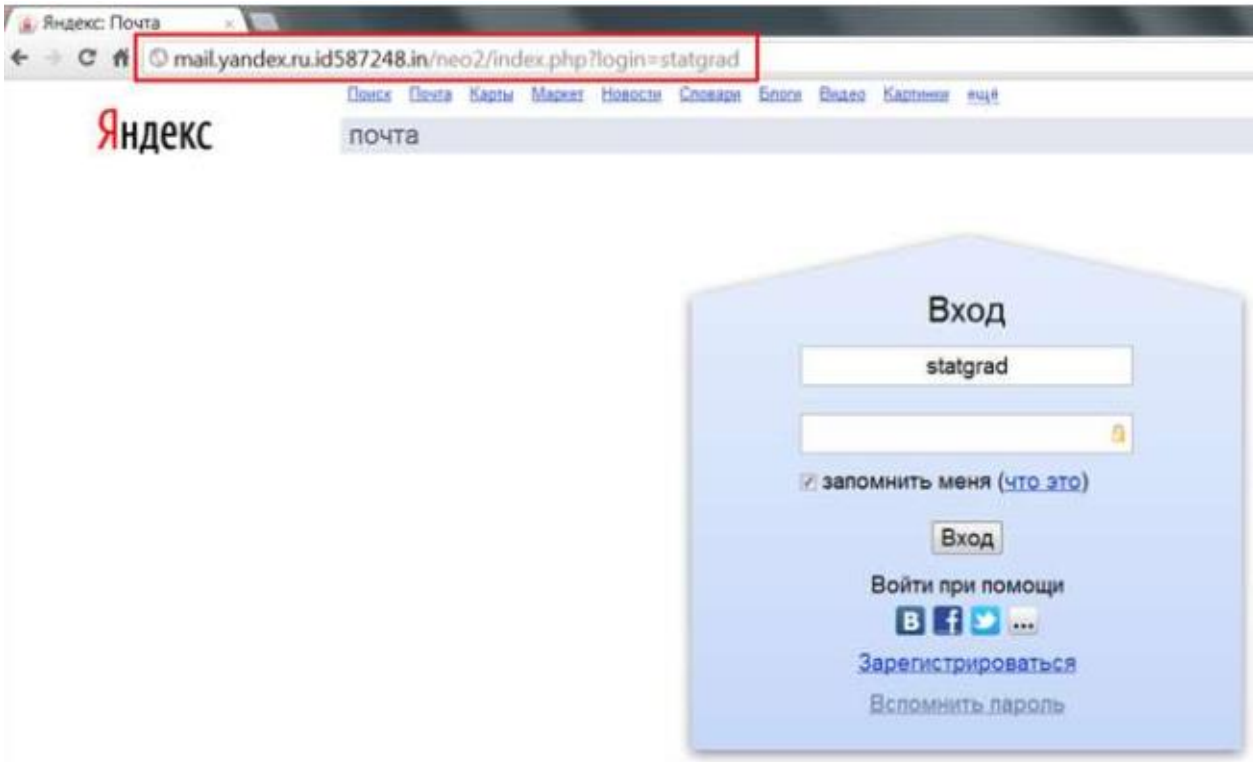
Правила безопасности при работе в сети:

1. Проверять адрес сайта
2. Блокировать компьютер
3. Проверять отправителя
4. Придумывать сложные пароли
5. Делать резервные копии ценных данных

1. Проверять адрес сайта

Внимательно читайте адрес сайта, на который вы перешли по ссылке. Вместо mail.yandex.ru может прийти похожая – mail.yandex.ru.id587248.in, это уже совсем иная страница, хотя ее внешний вид может полностью соответствовать оригиналу. Это так называемые «фишинговые сайты», предназначенные для похищения пароля.



Адрес в сети состоит из доменных имен разного уровня, разделенных точкой. Большинству популярных сайтов принадлежит имя второго уровня. (Например: Yandex.ru)

Yandex – доменное имя второго уровня.

Ru – доменное имя первого уровня, также называется зоной сети.

После имени первого уровня может идти только «/»!

До имени первого уровня могут располагаться имена других уровней, разделенные точкой. Имя второго уровня при этом не меняется!

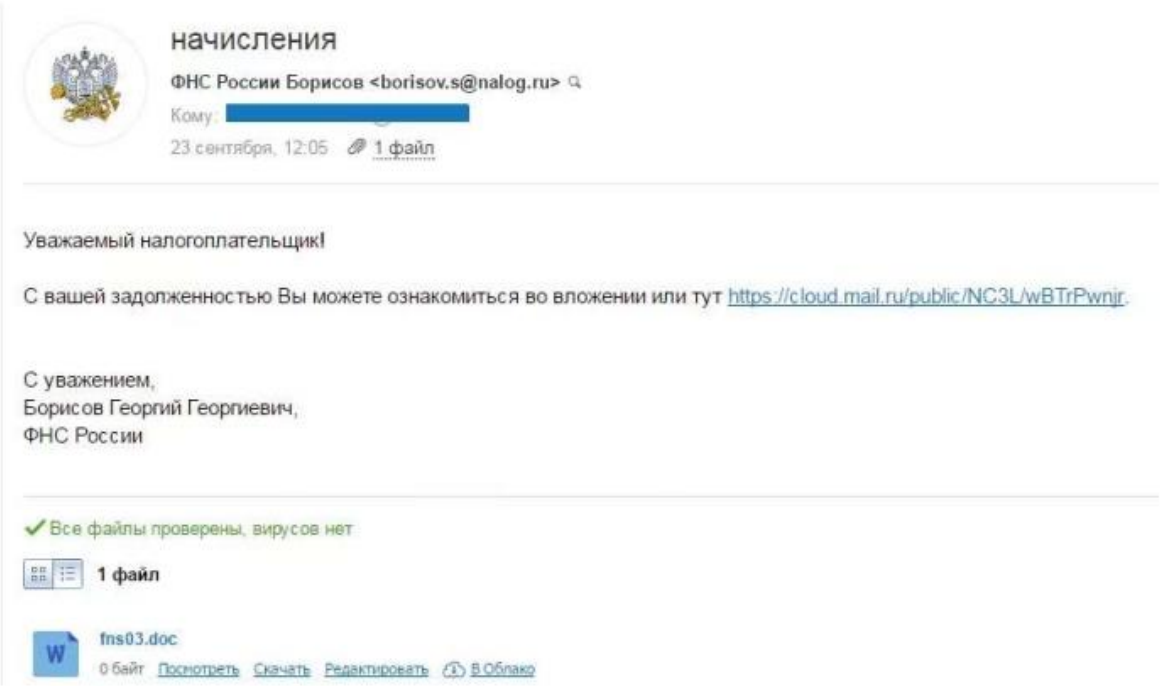
Во всех других случаях вас обманывают!

2. Блокировать компьютер

При каждом оставлении компьютера без присмотра – блокируйте. Заблокировать компьютер можно сочетанием клавиш Win+L

3. Проверять отправителя

Все видимые пользователю признаки официального письма легко подделать.



Не проходите сразу же по ссылкам, которые приходят вам в письмах. Для начала убедитесь, что они безопасны. Даже если сообщение пришло от знакомого человека, уточните у него, что за ресурс, куда он вас отправляет (ведь его аккаунт также могут взломать и выслать вам зараженные ссылки). То же касается и вложенных файлов в сообщениях. Не открывайте их, пока наверняка не узнаете об их «чистоте».

4. Придумывать сложные пароли

Хороший пароль содержит не меньше 8 символов, среди них — цифры, буквы и специальные символы: ! # $ % ^ { } [ ] ( ) " : \ |.
Не используйте простые сочетания вроде 123456, qwerty, password. Злоумышленники часто взламывают учетные записи, перебирая подобные варианты.

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 символах.

5. Делать резервные копии ценных данных

Вредоносные программы портят данные, шифруют жесткие диски и предлагают разблокировать их за деньги. Платить — значит финансировать разработку новых, еще более изощренных вирусов. Делайте резервные копии информации на других носителях. Подойдут CD, DVD, внешние диски, флеш-накопители, облачные сервисы.