***Для обеспечения информационной безопасности следуйте мерам предосторожности при работе в сети интернет:***

1. Ежедневно следите, чтобы Антивирус был обновлен и всегда Активен.

2. Не переходите по ссылкам на подозрительные ресурсы, сайты, программы.

3. Не запускайте программы, вложенные в письма, даже если они пришли к Вам от заведомо знакомого лица. Помните, что вирусы с легкостью могут подделать любой почтовый адрес и указать в письме ваши правильные личные данные, украв их из адресной книги вашего знакомого!

4. Перед запуском любой программы или открытии любого файла (в том числе реквизиты, документы) проверьте их антивирусной программой.

5. При работе с электронной почтой не открывайте письма и вложения к ним, полученные от неизвестных отправителей, не переходите по содержащимся в таких письмах ссылкам.

6. Если в поступившем письме содержится:

просьба ввести логин/пароль или создать логин/пароль при переходе по ссылке,

ссылка для перехода на сторонний сайт, который запрашивает доступ к вашему почтовому ящику от приложения или сайта,

ссылка для перехода на сторонний сайт, который запрашивает доступ к вашему почтовому ящику от приложения или сайта,

ни в коем случае не делайте этого!

Не передавайте никому Ваши логины/пароли, кроме как по письменному разрешению руководства (на бумаге) или устному запросу ваших коллег (по известному вам телефону или подойдите лично).

**7. Не распаковывайте архивы, если полностью не уверены в отправителе (лучше удостовериться, что он действительно его посылал, так как подделать почту очень просто, для этого не нужно даже ее взламывать). Архив должен сразу вызывать подозрения, особенно если написано, что там docx или pdf-документ.**

8.При работе с почтой ВСЕГДА смотрите на адрес отправителя, подделать почтовый адрес очень просто, для этого не нужно обладать какими-то особыми знаниями:

Он может быть похожим на настоящий, отличаться даже одной буквой. Например, вместо буквы o использована цифра 0 (ноль).