Памятка по безопасной работе с электронной почтой

1. Необходимо внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом.
2. Обращайте внимание на домен в адресе отправителя, если он не принадлежит организации, от имени которой написано письмо, а тем более если ящик зарегистрирован на бесплатных почтовых сервисах, то это верный признак мошеннического письма. Официальные рассылки всегда приходят с официальных адресов.
3. Следует с осторожностью относиться к письмам от неизвестных адресатов, ни в коем случае не открывать вложения и не переходить по ссылкам.
4. Следует проверять ссылки, даже если письмо получено от коллеги. Нужно помнить, что коллегу или знакомого могли взломать.
5. Признаки фишинговых ссылок, которые могут быть отправлены в почте:
   - посторонние домены, не относящиеся к организациям;
   - при наведении курсора мышки на ссылку всплывающий адрес не совпадает с написанным;
   - ошибки в написании;
   - автоматически сгенерированные последовательности символов в адресе ссылки;
   - символы из других языков, похожие на базовую латиницу — ç вместо c, á вместо a и так далее;
   - даже если ссылка содержит в себе «https:/», это не дает гарантии в ее безопасности.
6. Рекомендуем с подозрением относиться к письмам с вложениями, особенно если это документы с макросами, архивы с паролями, а также файлы с расширениями .rtf, .lnk, .chm, .vhd.
7. Рекомендуем с подозрением относиться к письмам с призывом к действиям (например «открой», «прочитай», «ознакомься»), а также к письмам, в темах которых упоминаются финансы, банки, геополитическая обстановка или содержатся угрозы.
8. Необходимо с подозрением относиться к письмам со ссылками, особенно если они длинные или, наоборот, созданы с помощью сервисов сокращения ссылок (например, bit.ly, tinyurl.com). Не переходить по ссылкам из письма, если они заменены на слова, наводить на них мышкой и просматривать полный адрес.
9. Следует с подозрением относиться к письмам на иностранном языке, особенно с орфографическими ошибками и с большим количеством получателей.
10. При получении писем, не соответствующих критериям безопасности, рекомендуем направлять их в папку «спам» и сообщать специалистам, ответственным за информационную безопасность.