Первоначальные действия при получении электронного письма

В последнее время участились случаи интернет-мошенничества и получения фишинговых* («писем с мошенническим содержанием») писем.

Фишинговые письма - письма мошеннического содержания (якобы от банка или других организаций), цель которых - заставить пользователей ввести конфиденциальную информацию для получения доступа к их данным.

Первоначальные действия при получении электронных писем:

Если вы получили письмо, в котором от Вас требуют какого-либо взаимодействия, в том числе, незамедлительного, или письмо вызывает у Вас любопытство, страх или побуждает к действиям, например, «открой»; «прочитай»; «ознакомься» и т.п., то задумайтесь и задайте себе следующие вопросы:

- ожидаю ли я это письмо?
- есть ли смысл в том, что от меня требуют?
- знаю ли я автора этого письма?
- уверен ли я в безопасности полученного письма?

Если ответ, хотя бы на один из вопросов «нет», то внимательно проанализируйте содержание письма и, при необходимости, свяжитесь для консультации с представителем технической службы поддержки.

ОБРАТИТЕ ОСОБОЕ ВНИМАНИЕ!

Для безопасности особого внимания требуют следующие письма:

- содержащие ссылку для перехода на сторонний ресурс (еще большего внимания заслуживают письма, содержащие «короткие ссылки», т.к. невозможно определить куда ведет такая ссылка);
- содержащие вложение (возможно, в файле содержится вредоносный код);
- составленные на иностранном языке;
- имеющие большое количество получателей;
- содержащие орфографические ошибки;
- связанные с финансовой или банковской сферой, геополитической обстановкой.