«Фишинг» – вид интернет-мошенничества, цель которого – получить идентификационные данные пользователей. Сюда относятся кражи паролей, номеров кредитных карт, банковских счетов и другой конфиденциальной информации.

Фишинг представляет собой пришедшие на почту поддельные уведомления от банков, провайдеров, платежных систем и других организаций о том, что по какой-либо причине получателю срочно нужно передать/обновить личные данные. Причины могут называться различные. Это может быть утеря данных, поломка в системе и прочее.

Как избежать фишинга?

1. Не доверяйте отображаемому имени.

Прежде чем открыть сообщение, проверьте адрес электронной почты отправителя – отображаемое имя может быть поддельным.

2. Проверьте сообщение на наличие опечаток.

Орфографические и грамматические ошибки типичны для фишинговых писем. Если что-то выглядит подозрительно, помечайте сообщение как спам.

3. Внимательно посмотрите, прежде чем щелкать.

Наведите курсор на гиперссылки, чтобы проверить адрес ссылки.

4. Читайте приветствие.

Если письмо адресовано не вам, а «дорогому клиенту», насторожитесь. Скорее всего, это мошенники.

5. Проверьте подпись.

Посмотрите, есть ли в подписи контактные данные. В письмах от безопасных отправителей чаще всего они есть.

6. Остерегайтесь угроз.

В фишинговых письмах часто встречаются фразы, основанные на страхе, такие как «Ваш счет был приостановлен».