

«Фишинг» – вид интернет-мошенничества, целью которого является получение конфиденциальных данных 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?

Не доверяйте отображаемому имени.

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

Проверьте сообщение на наличие опечаток.

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

Внимательно посмотрите, прежде чем щелкать курсором мыши.

Наведите курсор на гиперссылки, чтобы проверить адрес ссылки.

Читайте приветствие.

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

Проверьте подпись.

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

Остерегайтесь угроз.

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

[#МВД #МВД74 #Полиция74 #Челябинскаяобласть #МВДРоссии #Новости #ПолицияКатавИвановск#НеДайСебяОбмануть #Будьтебдительны](#)

