

Что такое фишинг? и как не попасть на уловки мошенников?

Отвечает помощник прокурора Пригородного района Гатагонов С.Р.

Фишинг является одним из видов интернет-мошенничества, используемый с целью получения неправомерного доступа к конфиденциальным данным человека.

С данной целью злоумышленники рассылают сообщения с вредоносными ссылками.

По ссылке Вас может ожидать вирус, троянская программа, фишинговый сайт, с помощью которых злоумышленники могут получить доступ к логинам и паролям, реквизитам банковской карты, данным об используемых устройствах и другим личным данным.

Мошенники могут прислать фишинговую ссылку, например, в сообщении в социальных сетях или мессенджере от имени незнакомого или знакомого человека, от имени реального интернет-магазина, интернет-сервиса, банка, государственного учреждения или другой организации.

Важно, что злоумышленники формулируют текст письма исходя из цели привлечения внимания, например:

«Ваш аккаунт заблокирован»

«Привет, это написано про тебя?»

«Отсылаю обещанные фотографии» и т.д.

Для защиты от фишинга необходимо не открывать сомнительные интернет-письма, потенциально опасные интернет-страницы, не загружать приложения к указанным письмам файлы, всегда проверять адрес электронной почты, с которой пришло интернет-письмо.

В каждом случае перехода на стороннюю интернет-страницу необходимо тщательно проверять подлинность ее электронного адреса, так как корректная ссылка настоящей интернет-страницы от фишинговой ссылки может отличаться одним или двумя похожими символами (например, а вместо о, і вместо l и др.).