Что такое «фишинг»? И как не стать его жертвой?

Фишингом называются атаки, когда злоумышленник связывается с человеком, выдавая себя за того, которого он знает, или за организацию, которой он доверяет, и пытается получить от него личные сведения или убедить открыть вредоносный веб-сайт или файл.

Чаще всего попытки фишинга осуществляются по электронной почте, но также могут использоваться SMS-сообщения, прямые сообщения в социальных сетях или даже телефонные звонки.

Как защититься от фишинга? Для этого необходимо соблюдать ряд рекомендаций.

Во-первых, необходимо внимательно изучать все сообщения, требующие каких-либо срочных действий. Обращать особое внимание на адрес электронной почты отправителя. Если сообщение утверждает, что оно из банка, но адрес отправителя не является его доменным адресом, это должно быть громким предупреждением.

Во-вторых, нельзя переходить по ссылкам и открывать вложения, полученные неожиданно, даже если они внешне выглядят как отправленные знакомым человеком или организацией. Лучше сразу же связаться с указанным отправителем и убедиться, что сообщение или вложение действительно отправлено именно им.

Кроме того, можно установить на персональные гаджеты специальные лицензионные программы, призванные блокировать известные фишинговые веб-сайты. Антивирусное программное обеспечение помогает защитить компьютер от спам-сообщений, а определитель номеров — от звонков, которые используют для фишинговых атак.

Главное правило – ни в коем случае не сообщать посторонним личные данные карты и не вводить их на незнакомых сайтах, не указывать коды безопасности из смс-сообщений.

Если возникло подозрение, что стали жертвой мошенников, следует незамедлительно обратиться в полицию.

Помощник прокурора Курского района В.Н. Рязанцева