Фишинг и способы защиты от него

Фишинг или по-другому кража личных данных – это вид интернет-мошенничества, который используется для тайного хищения конфиденциальных данных человека с помощью сайтов-подделок.

Суть данного способа мошенничества заключается в том, что на электронную почту или в SMS приходит письмо со ссылкой, по которой предлагается пройти для получения какого-либо блага. Эти действия совершаются чаще всего для того, чтобы получить доступ к банковским данным, либо к персональным данным лица. Обычно злоумышленники формулируют тему письма так, что на него хочется отреагировать, например: «Ваш аккаунт заблокирован», «Срочное сообщение от банка», «Вам необходимо срочно пройти по ссылке для восстановления данных» и т.п.

Чтобы распознать фишинговый сайт необходимо обратить внимание на следующее: в адресной строке нет https и значка закрытого замка, дизайн скопирован некачественно, в текстах сайта есть ошибки, а также на нем мало страниц или даже одна – для ввода данных карты.

Чтобы защититься от фишинга необходимо установить антивирус и регулярно обновлять его, сохранять в закладках адреса нужных сайтов, не переходить по подозрительным ссылкам, использовать отдельную карту для покупок в интернете.

В случае совершения в отношении вас мошеннических действий необходимо незамедлительно обращаться в правоохранительные органы.

Заместитель прокурора Рыльского района И.И. Милонова