Платные СМС-услуги: как не стать жертвой мошенниковВ последние годы интернет-мошенничество, называемое «фишинг», набирает обороты. Одним из видов мошенничества являются нежелательные подписки и платные СМС-услуги.Цель «фишинга»—получить доступ кличным даннымпользователя: логинам, паролям идругой информации.Мошенничество «фишеров» основано на незнании пользователями правил сетевой безопасности. Опасности могут подвергаться:1.Данные банковских карт. Если вы расплачиваетесь винтернете ихраните сбережения на одной итойже карте, подумайте, что случится, когда кто-то получит кней доступ.2.Логины ипароли ксервисам соплаченной подпиской. Купили годовую подписку на видеосервис? Оплатили доступ квиртуальной библиотеке? Ваш «читательский» могут украсть.3.Аккаунты всоциальных сетях. Даже если вы не топовый блогер смиллионами подписчиков, ваши логины ипароль представляют интерес для «фишеров»: например, их можно продать нелегальным накрутчикам лайков ирепостов или попросить от вашего имени деньги вдолг.4.Пароли от почтовых ящиков. Что хранит ваша рабочая или личная почта? Зачастую—всё, начиная от конфиденциальных документов, заканчивая аккаунтами винтернет-сервисах.Основной приём фишеров—имитация хорошо знакомых всем сайтов для получения сих помощью личной информации пользователей. Всплывающие баннеры самого разного содержания могут привести пользователя, например, на поддельную страницу авторизации всоциальной сети. Самый верный способ не попасться на крючок—внимательно смотреть на адресную строку. Любые отличия вимени домена должны остановитьпользователя.В случае возникновения сомнительных ситуаций необходимонезамедлительнообращаться в компанию-провайдер по телефонам, указанным на официальном сайте, либо через личный кабинет абонента в официальном приложении.Для исключения последствий атак злоумышленников, операторами внедряются сервисы блокировки нежелательного контента и развлекательных подписок