Платные СМС-услуги: как не стать жертвой мошенников

В последние годы интернет-мошенничество, называемое «фишинг», набирает обороты. Одним из видов мошенничества являются нежелательные подписки и платные СМС-услуги.
Цель «фишинга» — получить доступ к личным данным пользователя: логинам, паролям и другой информации.
Мошенничество «фишеров» основано на незнании пользователями правил сетевой безопасности.

Опасности могут подвергаться:

1. Данные банковских карт. Если вы расплачиваетесь в интернете и храните сбережения на одной и той же карте, подумайте, что случится, когда кто-то получит к ней доступ.
2. Логины и пароли к сервисам с оплаченной подпиской. Купили годовую подписку на видеосервис? Оплатили доступ к виртуальной библиотеке? Ваш «читательский» могут украсть.
3. Аккаунты в социальных сетях. Даже если вы не топовый блогер с миллионами подписчиков, ваши логины и пароль представляют интерес для «фишеров»: например, их можно продать нелегальным накрутчикам лайков и репостов или попросить от вашего имени деньги в долг.
4. Пароли от почтовых ящиков. Что хранит ваша рабочая или личная почта? Зачастую — всё, начиная от конфиденциальных документов, заканчивая аккаунтами в интернет-сервисах.

Основной приём фишеров — имитация хорошо знакомых всем сайтов для получения с их помощью личной информации пользователей. Всплывающие баннеры самого разного содержания могут привести пользователя, например, на поддельную страницу авторизации в социальной сети.

Самый верный способ не попасться на крючок — внимательно смотреть на адресную строку. Любые отличия в имени домена должны остановить пользователя.

В случае возникновения сомнительных ситуаций необходимо незамедлительно обращаться 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.