Как не стать жертвой фишинга

Фишинг — вид интернет-мошенничества, цель которого получить доступ к секретным данным пользователя: логинам и паролям, номерам карт, банковским счетам. Преступники присылают фишинговые письма, которые могут быть очень похожи на настоящие сообщения от банков, компаний, органов власти или Госуслуг. Но ссылка в таком письме ведёт на поддельный сайт. Став жертвой фишинга, можно лишиться денег или доступа к своим аккаунтам, пустить хакера в корпоративную сеть работодателя. Фишинговыми бывают не только письма, приходящие на электронную почту. Это могут быть сообщения в мессенджерах, социальных сетях и смс. Рассказываем, как распознать и защититься от фишинга

Поддельные приложения

Мошенники используют в своих схемах приложения для смартфонов, планшетов и компьютеров. Эти программы содержат вирусы, которые крадут банковские реквизиты, логины и пароли от мобильног или онлайн-банка, а также перехватывают смс с кодами. Чаще подделывают мобильные банки — если ввести логин и пароль, хакеры получат доступ к вашим счетам в настоящем приложении

Письмо с выгодным предложением

Киберпреступники рассылают письма от имени интернет-магазинов, сервисов доставки еды и брокерских контор. Ссылки из таких писем ведут на поддельные сайты, которые похожи на настоящие. Цель преступников — заставить вас поверить, что это реальный магазин, сервис, брокер, чтобы вы совершили покупку онлайн. Никаких товаров и услуг вы не получите, а мошенники скроются с вашими деньгами

Письмо от отдела кадров, ИТ-департамента, партнёров или подрядчиков

Мошенники имитируют письма от ваших коллег, клиентов или подрядчиков. Письмо может содержать ссылку на фишинговый сайт или вложение с вредоносной программой. Цель хакеров — получить доступ к вашей рабочей учётной записи или заразить вирусом корпоративный компьютер. Это может стать началом кибератаки на вашего работодателя

Сообщение о необходимости смены пароля

Злоумышленники имитируют письма от администрации социальных сетей, интернет-магазинов. В письмах просят пользователя сменить пароль. При переходе по ссылке вы окажетесь на сайте, который оформлен как настоящий интернет-сервис. На странице предложат ввести старый пароль и придумать новый. Так действующий пароль от вашего аккаунта окажется у мошенников