Как не стать жертвой фишинга

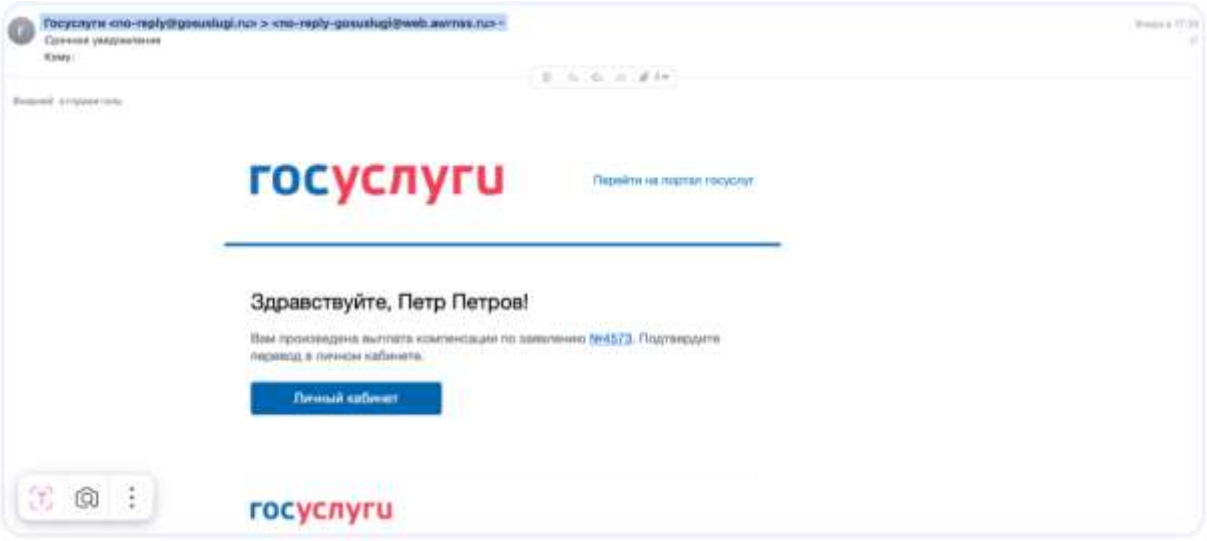
Фишинг — вид интернет-мошенничества, цель которого получить доступ к секретным данным пользователя: логинам и паролям, номерам карт, банковским счетам. Преступники присылают фишинговые письма, которые могут быть очень похожи на настоящие сообщения от банков, компаний, органов власти или Госуслуг. Но ссылка в таком письме ведёт на поддельный сайт. Став жертвой фишинга, можно лишиться денег или доступа к своим учётным записям, 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. Узнайте, как распознать и защититься от фишинга

В 2023 году выявлено более 40 тыс. доменных имён и ресурсов, которые потенциально могут использоваться для организации фишинговых атак. Подтверждённые факты фишинга отмечены в 17% случаев. Число выявленных фишинговых ресурсов выросло по сравнению с 2022 годом на 21%

Примеры фишинга

Сообщение о выигрыше или назначенной выплате от государства

При переходе по ссылке откроется поддельный сайт, на котором вам предложат ввести данные банковской карты для получения выигрыша. Так мошенники получат доступ к вашей карте и могут списать с неё все деньги. Иногда сайты, на которые ведёт ссылка из сообщения, заражены вирусами и пытаются загрузить на ваше устройство вредоносные программы



Сообщение о необходимости смены пароля

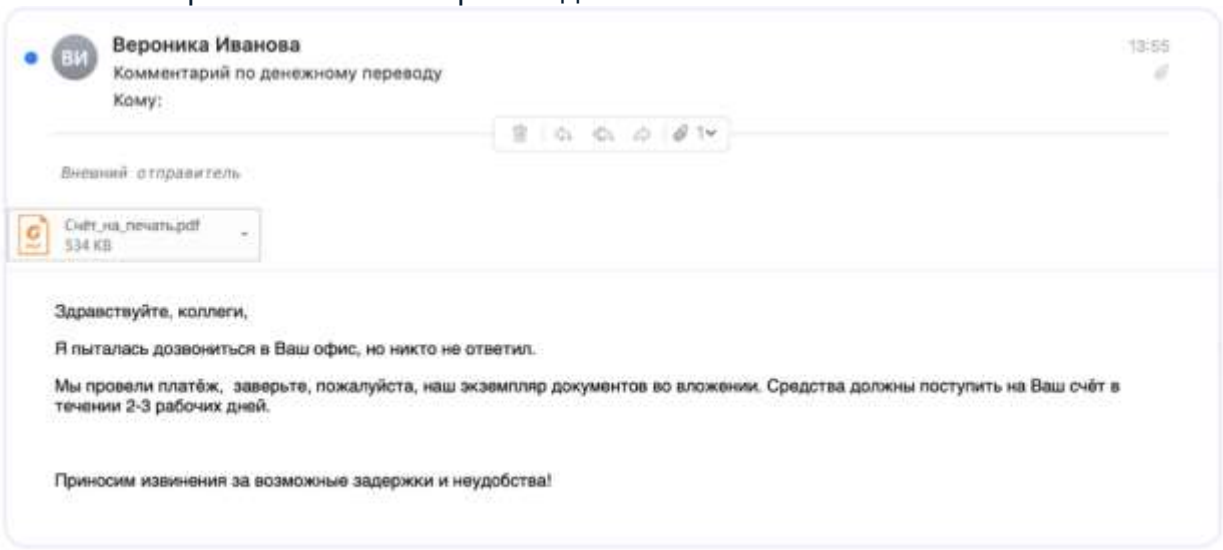
Злоумышленники имитируют письма от администрации социальных сетей, интернет-магазинов. В письмах просят пользователя сменить пароль. При переходе по ссылке вы окажетесь на сайте, который оформлен как настоящий интернет-сервис. На странице предложат ввести старый пароль и придумать новый. Так действующий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

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

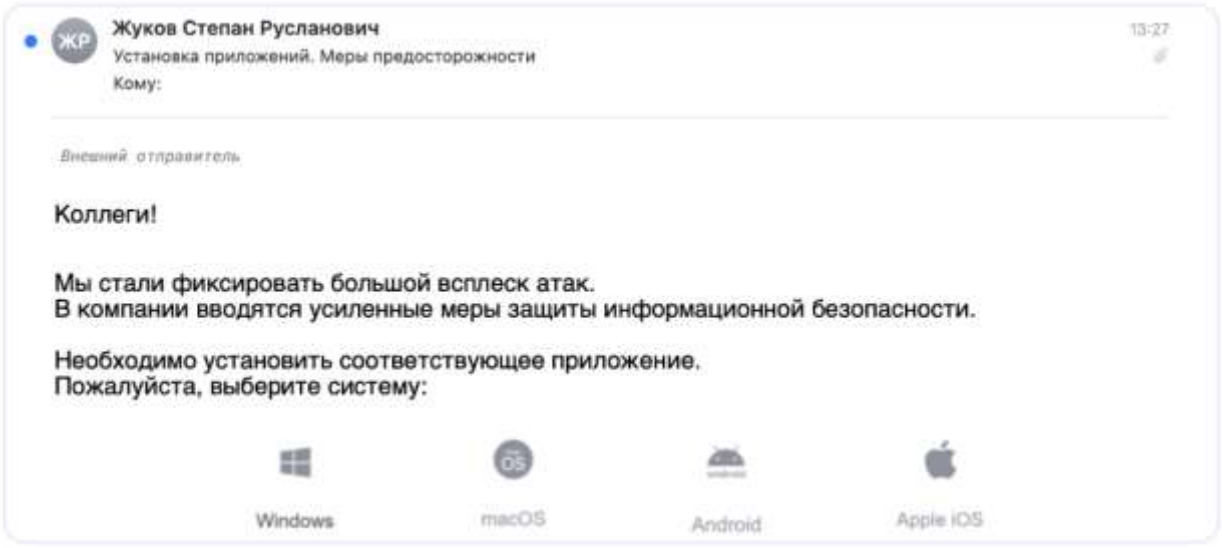
Письмо от отдела кадров, ИТ-департамента, партнёров или подрядчиков

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



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 мобильного 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



Как защититься от фишинга

Внимательно проверяйте адрес отправителя

Адрес сайта может отличаться от настоящего всего одной буквой, символом или доменом. Проанализируйте адрес сайта, на который были переадресованы. Например, он может заканчиваться на .com вместо .gov. или иметь вид https://www.gossuslugi.ru/ вместо https://www.gosuslugi.ru/ с двойной «s»

Не переходите по подозрительным ссылкам в сообщениях

Получив сообщение на почту, в соцсети, мессенджер, не переходите по ссылкам из писем, если вы их не запрашивали. Уведомление из банка или от онлайн-магазина можно проверить, позвонив по телефону с официального сайта
С подозрением относитесь к рекламным баннерам на сайтах — они могут вести на фишинговый сайт или содержать в себе вредоносный код

Проверяйте информацию из рассылок

Если в письме пришло приглашение принять участие в акции компании, проверьте информацию на её официальном сайте, который найдёте через поисковик. Это касается и ситуации, когда вам сообщают о новых выплатах — всю информацию о них можно найти на официальных сайтах органов власти или на Госуслугах

Меняйте пароли в самом сервисе

Не переходите по ссылкам о смене пароля или других учётных записей, чтобы поменять их. При необходимости меняйте пароли через личный кабинет, а не по ссылке из соответствующего письма. Не путайте смену пароля с ситуацией восстановления пароля, когда вы сами запрашиваете ссылку, которая придёт в письме

Скачивайте программы из официальных магазинов приложений

Обращайте внимание на количество скачиваний, рейтинг и отзывы. Если программа совсем новая и её пока мало кто установил, лучше не рисковать. Смотрите отзывы не только в магазине приложений, но и на профильных форумах. Так вы узнаете, не возникало ли проблем с программой в последнее время
Если необходимо установить приложения банков, попавших под санкции, скачайте их с официальных сайтов организаций

Сообщайте о подозрительных письмах на рабочей почте службе безопасности или ИТ-отделу

Прежде чем перейти по ссылке из такого письма или открыть вложение, созвонитесь с отправителем и узнайте, действительно ли это письмо от него

Повышайте киберграмотность

Проверяйте свои знания, чтобы понять, насколько хорошо вы умеете распознавать фишинг. С этим помогут тесты по кибербезопасности. При необходимости пройдите курсы цифровой безопасности, иногда такое обучение устраивает работодатель