Интернет-мошенничество и как от него защититься?

Фишинг (от английского fishing – рыбная ловля) – вид интернет-мошенничества для получения доступа к личным данным пользователя: логинам и паролям, номерам карт, банковским счетам.

Наиболее распространенная тактика фишинга выглядит следующим образом. Пользователь получает электронное письмо, которое внешне может быть очень похоже на настоящее сообщение от популярных организаций: банков, компаний, органов власти или госуслуг. Если пользователь «клюет на наживку» и переходит по ссылке из письма, он попадает на поддельный сайт, внешне неотличимый от настоящего. Введенные на этом сайте данные отправляются напрямую к злоумышленникам, которые затем используют их для кражи персональной информации или денег с банковских счетов. Фишинговыми бывают не только письма, приходящие на электронную почту. Это могут быть сообщения в мессенджерах, социальных сетях и смс.

Сообщение о выигрыше или назначенной выплате от государства

Если вам пришло письмо с сообщением о внезапном выигрыше или информацией о назначенной мере соцподдержки, о которой вы впервые слышите, будьте внимательны – это распространенный прием фишинга. При переходе по ссылке из письма открывается фейковый сайт, на котором вам предложат ввести данные банковской карты для получения выигрыша или выплаты. Так мошенники получат доступ к вашей карте и смогут списать с нее все деньги.

Что делать?

Доверяйте только той информации, которая размещается на госуслугах или на официальных сайтах органов власти.

Сообщение о необходимости смены пароля

Часто злоумышленники имитируют письма от администрации социальных сетей, интернет-магазинов и популярных сервисов. В этих письмах они сообщают о том, что пароль устарел, больше не является безопасным, и просят пользователя его сменить. При переходе по ссылке открывается сайт, который оформлен как настоящий интернет-сервис. На странице предлагается ввести старый пароль и придумать новый. Если вовремя не проявить бдительность, можно передать действующий пароль от вашего аккаунта в руки мошенников.

Что делать?

Не переходите по ссылкам о смене пароля или других учетных записей, чтобы поменять их. При необходимости меняйте пароли через личный кабинет, а не по ссылке из письма. Не путайте смену пароля с его восстановлением, при котором вы сами запрашиваете ссылку на электронную почту.

Письмо с выгодным предложением

Киберпреступники могут рассылать письма от имени интернет-магазинов или сервисов доставки еды с информацией об очень выгодном предложении или акции. Ссылки из таких писем ведут на поддельные сайты, внешне похожие на настоящие. Цель обманщиков – заставить вас поверить,

что это реальный магазин или сервис, чтобы вы совершили покупку онлайн. Никаких товаров и услуг вы не получите, а мошенники скроются с вашими деньгами.

Что делать?

Если вас приглашают принять участие в акции компании, перейдите на официальный сайт интернет-магазина самостоятельно или позвоните на горячую линию компании и уточните, существует ли такое предложение в действительности.

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

Письма приходят якобы от ваших коллег, клиентов или подрядчиков, нередко с пометкой «важно» или «срочно». Такие письма содержат ссылку на фишинговый сайт или вложение с вредоносной программой. Цель хакеров – получить доступ к вашей рабочей учетной записи или заразить вирусом корпоративный компьютер. Это может стать началом кибератаки на вашего работодателя.

Что делать?

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

Поддельные приложения

В своих схемах мошенники используют приложения для смартфонов, планшетов и компьютеров. Эти программы содержат вирусы, крадут логины и пароли от онлайн-банка, а также перехватывают смс с кодами. Чаще всего подделывают приложения мобильных банков – если ввести логин и пароль в такой программе, хакеры получат доступ к вашим счетам в настоящем приложении.

Что делать?

Скачивайте программы из официальных магазинов приложений, обращая внимание на количество скачиваний, рейтинг и отзывы. Если программа совсем новая и ее пока мало кто установил, лучше не рисковать. Если необходимо установить или обновить приложения банков, попавших под санкции, скачивайте их с официальных сайтов организаций.

Чтобы обеспечить свою безопасность и не стать жертвой интернет-мошенников.

- Внимательно проверяйте адрес отправителя.
- Ищите информацию об акциях или выплатах на официальных сайтах компаний и ведомств.
- Изменяйте учетные данные не по ссылке из письма, а самостоятельно зайдя на сайт.
- Не переходите по подозрительным ссылкам.
- Не открывайте присланные файлы, если не уверены в отправителе.
- Не устанавливайте приложения из сомнительных источников.
- Будьте бдительны и повышайте киберграмотность.