Банк России зафиксировал случаи рассылки email-сообщений, содержащих недостоверную информацию о запуске национальной платежной системы «Мир».

Подобные сообщения содержат описание возможностей платежной системы «Мир» и предложение получить карты данной платежной системы, заполнив форму участника, находящуюся во вложении. При этом имеющийся во вложении исполняемый код позволяет злоумышленникам загружать на компьютер клиента вредоносное программное обеспечение различной направленности.

Фишинговые email-сообщения рассылаются от имени крупных кредитных организаций. При этом адрес отправителя email-сообщения по признакам может принадлежать существующей кредитной организации. В то же время одна из отличительных особенностей таких email-сообщений — перечисление в тексте заведомо большого количества преимуществ данной платежной системы, в том числе прямого доступа к криптовалютам.

Подобного рода email-рассылки Банк России расценивает как новый вид мошенничества.

Банк России призывает граждан — получателей таких фишинговых сообщений не открывать содержащиеся в них вложения и не пересылать их, а также предлагает кредитным организациям довести данную информацию до своих клиентов.

При получении подобных email-сообщений Банк России рекомендует гражданам ставить об этом в известность клиентскую службу кредитной организации, от лица которой получено сообщение. Источник: ЦБ РФ

Фи́шинг (англ. *phishing*, от *fishing* — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее. Источник: Википедия