«Оформите возврат страховых накоплений по ссылке»

Раиса, Барнаул

«Получила на мейл письмо, что мне по закону N 167-ФЗ начислен возврат страховых накоплений. Некая Луиза из неведомой «службы фин. мониторинга» написала, что из-за технических проблем денежный перевод еще до меня не дошел и теперь мне нужно самой его завершить. Для этого надо нажать в письме кнопку «Оформить возврат» и следовать инструкциям.

Прилагается некий уникальный номер перевода – какой-то набор букв и цифр. Видимо, «по инструкции» его нужно будет где-то ввести. И приписка внизу: не получится сделать все онлайн – идите в МФЦ с полным пакетом документов. Видимо, так они пытались придать хоть какую-то правдоподобность своим словам.

Было нетрудно догадаться, что это развод: письмо без темы, прислано с какой-то обычной почты на яндексе. Что за «служба фин. мониторинга» и что они мониторят, не уточняется. Догадываюсь, что просто охотятся на дурачков и чужие деньги.

По ссылке переходить не стала, от греха подальше письмо переложила в спам, где ему и место. Будьте осторожны!»

Совет эксперта по противодействию мошенничеству:

Социальные инженеры, составившие фейковую рассылку, надеялись, что Раиса поверит в историю с законом и перейдет по ссылке на фишинговый сайт. Затем «по инструкции» введет на странице полные данные своей банковской карты, включая срок действия и три цифры с оборота, якобы для получения своих накоплений. Или оплатит картой комиссию за перевод.

Сделав это, Раиса открыла бы мошенникам доступ к своему счету, и они смогли бы его опустошить. Банки ничего не возвращают, если клиент нарушил правила безопасности – ввел данные карты на фальшивом сайте или перевел деньги мошенникам.

Подобные «письма счастья» – не редкость. Чтобы внушить доверие, аферисты ссылаются на законы – чаще всего выдуманные – и упоминают в своих сообщениях известные организации – МФЦ, налоговую службу, пенсионные фонды, Банк России и другие.

Ни в коем случае нельзя переходить по ссылкам из подозрительных сообщений – за ними могут скрываться как фишинговые страницы, так и вирусы, которые украдут данные с вашего телефона, планшета или компьютера. Лучше сразу удалять сомнительные письма.

Получив уведомление о выплате, всегда перепроверяйте информацию. Найдите в официальных источниках документы, на которые ссылаются авторы письма. Проясните ситуацию в организации, которая фигурирует в сообщении. Но не стоит звонить по номеру из рассылки – вероятнее всего, по нему вас поджидают мошенники. Найдите номер организации на ее официальном сайте.