РЕКОМЕНДАЦИИ
по противодействию актуальным угрозам безопасности информации

Настоящие рекомендации направлены на повышение осведомленности о методах действий злоумышленников в интернет-пространстве в целях исключения рисков их негативного воздействия на производственные процессы компании и причинения вреда работникам ОАО «РЖД».

1. Об объектах интернет-мошенничества

Все информационные системы ОАО «РЖД» – это объекты критической информационной инфраструктуры, а значит, они являются привлекательными целями для киберпреступников, которые стремятся нанести вред как непосредственно ОАО «РЖД», так и в целом Российской Федерации. Сценарии их действий постоянно совершенствуются, становятся сложными и многоступенчатыми.

Профиль ставшего объектом их внимания подразделения (например, железной дороги, функционального филиала, подконтрольного общества и пр.) внимательно изучается, а именно: направления деятельности, состав руководства и персонала. Анализируется публичная информация не только из официальных источников, но и личных страниц работников в социальных сетях.

В этой связи излишняя активность в социальных сетях является распространенной ошибкой работников, которая может стоить компании как больших финансовых потерь, так и репутации. Большую часть информации о будущих жертвах злоумышленники, берут из открытых профилей, в которых работниками компаний размещаются фото и видео с корпоративных праздников, совместного отдыха с коллегами и пр.

Такие «цифровые следы» позволяют легко найти контакты потенциальной жертвы, составить ее психологический портрет, круг общения и выбрать соответствующий метод воздействия с широким использованием возможностей социальной инженерии.

Так, особое внимание мошенников обращено на работников, которые в рамках служебных обязанностей осуществляют внешнее взаимодействие – в первую очередь, это службы управления персоналом, корпоративных коммуникаций, бухгалтерия.

В качестве примера можно привести следующие сценарии:

- направление специалисту службы управления персоналом письма от соискателя на должность либо наоборот – на электронную почту работника

от лица кадрового подразделения другой компании с предложением более выгодной вакансии. В оба вида писем киберпреступники добавляют вредоносные ссылки или вложения под видом резюме или описания вакансии;

- использование специализированных рекрутинговых платформ, где присутствуют данные как работодателей, так и сотрудников различных компаний. Злоумышленник создает фальсифицированную страницу на сервисе либо взламывает существующую, принадлежащую сотруднику другой компании, и связывается с намеченной жертвой через внутреннюю систему такого сервиса. Его цель — установить доверие, расположить к себе человека, чтобы он поверил, что говорит с коллегой или потенциальным работодателем, и перешел по вредоносной ссылке в присланном впоследствии письме;

- направление работнику бухгалтерии или службы управления персоналом письма якобы от регулятора, в котором сообщается о проводимой проверке в связи с действиями работников компании (заявки на кредит, финансовые правонарушения, предоставление данных воинского учета и т.п.). Зачастую в письме мошенники просят адресата дождаться звонка якобы от инспектора, который предоставит более подробную информацию. Но на самом деле «инспектор» попытается собрать сведения конфиденциального характера, которые в дальнейшем использовать для проникновения в корпоративную сеть.

2. Об основных методах фишинга

Задачи большинства фишинговых рассылок, направленных на корпоративных пользователей – либо получение доступа к рабочей почте, либо попытка заразить рабочее устройство вредоносным программным обеспечением. Для достижения этих целей используются несколько типовых методов:

- использование в фишинговых письмах вложений в виде ссылок на вредоносные файлы, замаскированных под документы с расширениями .doc, .docx или .pdf;

- направление сообщений с вложениями в виде вредоносных QR-кодов. В отличие от обычных ссылок обнаружить их сложно, так как визуально мошеннический код не отличается от любого другого;

- имитация писем от государственных, в том числе правоохранительных органов. В этом случае почтовый адрес отправителя может быть похож на реальный, но отличаться несколькими символами, а вредоносное вложение маскируется под официальный документ, зачастую адресованный в одно из подразделений ОАО «РЖД».

3. О рисках реализации угроз безопасности информации

Деструктивное воздействие на информационные системы ОАО «РЖД» в случае успеха может привести к значительным негативным последствиям в экономической и социальной сфере – от нарушения перевозочного процесса и недоступности транспортных услуг до ущерба жизни и здоровью людей. В таком результате в условиях специальной военной операции на Украине заинтересованы, в первую очередь, специальные службы недружественных государств, под патронажем которых работают целые группировки киберпреступников.

При этом остается актуальным и более привычный интерес злоумышленников – проникновение во внутренний периметр компании в целях заражения вирусом-вымогателем, шифрующим данные, с которыми работает организация или ее подразделение. В таких ситуациях обычно требуют выкуп, который может исчисляться суммами до нескольких миллионов долларов, в зависимости от масштаба финансового оборота организации.

Также корпоративные данные могут быть похищены злоумышленниками с целью шантажа их опубликованием. В этом случае финансовые потери могут кратно возрасти вследствие штрафов от регуляторов, а атакованная компания несет серьезные репутационные потери. Важно понимать, что уплата выкупа не останавливает мошенников, сохраняющих анонимность, в реализации их угроз.

4. Рекомендации по противодействию угрозам

Получив любое письмо, важно читать его внимательно и не спешить переходить по ссылкам.

Особо критичного отношения требуют письма, содержащие призывы к действиям (например, «открой», «прочитай», «ознакомься»), с темами про банки, геополитическую обстановку или угрозы, письма на иностранном языке, с большим количеством получателей и орфографическими ошибками, а также если речь в них идет о предоставлении корпоративных или персональных данных и финансовых операциях.

Во всех случаях следует:

- проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
- не переходить по содержащимся в письме ссылкам, даже если оно получено якобы от работника ОАО «РЖД»;
- осуществлять проверку всех прикрепленных файлов средствами антивирусной защиты актуальных версий.

Взвешенное поведение – залог безопасности:

- не следует использовать интернет - ресурсы, если это не связано с выполнением служебных обязанностей;

- при осуществлении внешнего взаимодействия в служебных целях необходимо проявлять особую бдительность, своевременно распознавать признаки применения социальной инженерии;

- запрещается передавать персонифицированные учетные записи и соответствующие им пароли от информационных систем третьим лицам, в том числе другим работникам ОАО «РЖД»;

- недопустимо использование автоматической переадресации электронных писем из электронной почтовой системы ОАО «РЖД» на внешние адреса электронной почты (в том числе личные);

- запрещается публиковать или указывать в качестве обратной связи в социальных сетях корпоративные адреса электронной почты ОАО «РЖД» и служебные телефоны;

- ведение личных страниц в социальных сетях должно осуществляться в соответствие с Кодекса деловой этики ОАО «РЖД».

Кодекса деловой этики ОАО «РЖД». Содержание пункта «Поведение в социальных сетях и цифровом пространстве».

Интернет дает уникальные возможности для общения и обмена информацией, но требует ответственного отношения. Мы должны соблюдать определенные принципы и нормы поведения в социальных сетях.

Необходимо помнить, что любая публикация в сети Интернет носит публичный характер и влияет на репутацию компании.

При использовании социальных сетей и каналов обмена информацией мы:
- не используем корпоративную почту в личных целях;
- не раскрываем информацию о клиентах и партнерах;
- используем специальные каналы обратной связи для предложений по улучшению работы подразделений и избегаем негативных оценок в адрес компании в социальных сетях;
- не размещаем фотографии, аудио- и видеозаписи с корпоративных мероприятий, рабочих мест и производственных объектов, которые нарушают правила безопасности, могут нанести урон репутации компании и отдельным работникам;
- не публикуем информацию конфиденциального характера и иную служебную информацию, доступ к которой получили в рамках выполнения своих рабочих обязанностей;
- исключаем публичные призывы к осуществлению деятельности,

направленной против безопасности государства, а также случаи распространения заведомо ложной информации и дискредитации государственной власти;
- можем публиковать на личных страницах в социальных сетях общедоступную информацию о деятельности компании, положительно влияющую на репутацию ОАО "РЖД".

Наша информационная политика предусматривает раскрытие всех необходимых сведений о нашей деятельности в открытых источниках.

БУДЬТЕ БДИТЕЛЬНЫ!