СОБЛЮДАЙТЕ ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ОСТЕРЕГАЙТЕСЬ ФИШИНГОВЫХ САЙТОВ

1 http://rjd.ru ✕

ОБРАЩАЙТЕ ВНИМАНИЕ НА
название сайта в адресной строке, на котором вводите учетные данные (логин, пароль или пин-код) — мошенники могут использовать ссылки на поддельные страницы, чтобы собрать информацию о вас.

2 ivanovaa@center.rjd.ru ✕

ВНИМАТЕЛЬНО ПРОВЕРЯЙТЕ
адрес отправителя электронного письма, даже если на первый взгляд он совпадает с уже известным контактом.

3 http://www.vtb_pay.ru ✕

ПРОВЕРЯЙТЕ
ссылки в письмах или сообщениях, в том числе — от коллег и знакомых. Помните, их электронную почту или аккаунт в мессенджере могли взломать.

4

ОТНОСИТЕСЬ С ОСТОРОЖНОСТЬЮ
к письмам с призывом к действию

НАПРИМЕР:

открой | прочитай | ознакомься

или темами про финансы, банки, геополитическую обстановку и угрозы.

ФИШИНГ – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям.

5

ЕСЛИ ВЫ ПОЛУЧИЛИ НА КОРПОРАТИВНУЮ ПОЧТУ ПОДОЗРИТЕЛЬНОЕ ПИСЬМО

КАК ОНО МОЖЕТ ВЫГЛЯДЕТЬ:

- ✕ от неизвестного отправителя
- ✕ подозрительная ссылка или вложение
- ✕ требование срочного ответа
- ✕ грамматические или лексические ошибки в тексте
- ✕ просьба предоставить данные для получения денежного вознаграждения

- ✓ **НЕ** отвечайте на него
- ✓ **НЕ** предоставляйте никакую информацию
- ✓ **НЕ** переходите по ссылке
- ✓ **НЕ** открывайте вложения
- ✓ **ОТПРАВЬТЕ** подозрительное письмо по адресу info-soc@gvc.rzd
- ✓ **УДАЛИТЕ** подозрительное письмо

ЗАЩИТИТЕ ДАННЫЕ НА СМАРТФОНЕ

- ✓ **Я ДОВЕРЯЮ** разработчику приложения
- ✓ **Я ВКЛЮЧИЛ** push-уведомления в банковских приложениях
- ✓ **Я РАЗРЕШАЮ** приложению доступ только к необходимым данным в смартфоне
- ✓ **Я НЕ ПЕРЕХОЖУ** по подозрительным ссылкам из СМС, календарей или мессенджеров

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ РАБОТЕ НА ПК

1

НЕ ПОЗВОЛЯЙТЕ
третьим лицам просматривать служебную информацию на вашем компьютере.

2

ОБЯЗАТЕЛЬНО ПРОВЕРЯЙТЕ
на вирусы любой съемный носитель информации при его подключении.

3

НЕ ЗАГРУЖАЙТЕ И НЕ ОТКРЫВАЙТЕ
служебные документы на личном компьютере.

4

НЕ ПОДКЛЮЧАЙТЕ
к рабочему компьютеру USB-модем и мобильные устройства: смартфон, планшет и другую технику.

ПРАВИЛА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ЦИФРОВЫХ КОММУНИКАЦИЯХ

1

✓

ИСПОЛЬЗУЙТЕ только корпоративные сервисы для общения с коллегами по рабочим вопросам

- ЕКС МОС на базе мессенджера eXpress для мгновенных сообщений
- КСОФ на базе Mflash для данных большого объема

✗

НЕ ИСПОЛЬЗУЙТЕ иностранные сервисы, а также технику компании Apple для обмена служебной информацией

Gmail.com, Google Drive, Icloud.com, WhatsApp*, Telegram и др.

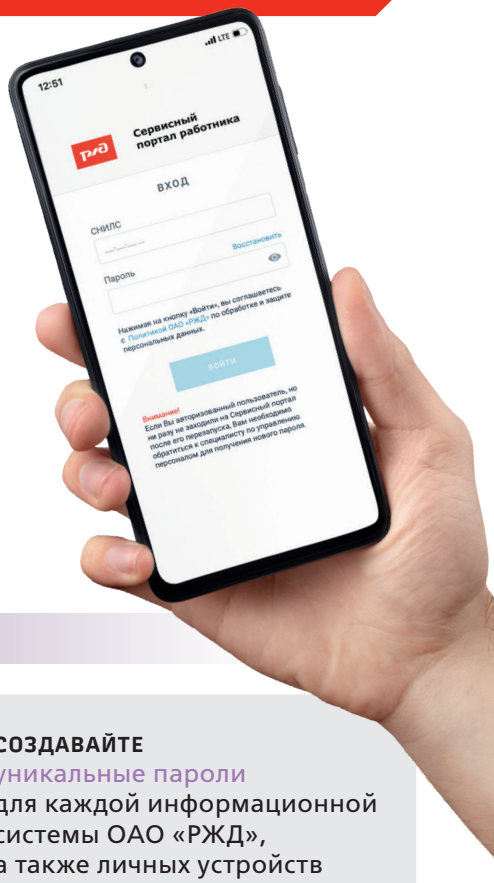
*принадлежит корпорации Meta, признанной экстремистской и запрещенной в России

2

НЕ РАЗМЕЩАЙТЕ служебную информацию в открытых источниках, например, в социальных сетях или на форумах.

3

ПОЛЬЗУЙТЕСЬ корпоративной электронной почтой только для выполнения производственных задач, **НЕ УКАЗЫВАЙТЕ ЕЕ** при регистрации в сторонних сервисах или как способ обратной связи с вами.



4

ПРОВЕРЯЙТЕ на вирусы все файлы, поступившие по электронной почте и из социальных сетей.

5

НЕ ПУБЛИКУЙТЕ в социальных сетях фотографии личных документов

паспорта, водительских прав, служебного удостоверения или пропуска.

ПАРОЛЬ ДОЛЖЕН БЫТЬ НАДЕЖНЫМ

1

ПАРОЛЬ ДОЛЖЕН СОДЕРЖАТЬ

- ✓ не менее 12 символов
- ✓ прописные и строчные буквы a-z, A-Z
- ✓ цифры и специальные символы &*!% и т.п.

3%nqIkNR!p2wTe5

Сверяйте их со списками популярных паролей, публикуемых в открытых источниках.

2

СОЗДАВАЙТЕ уникальные пароли для каждой информационной системы ОАО «РЖД», а также личных устройств и аккаунтов в интернет-сервисах.

3

ИСПОЛЬЗУЙТЕ двухфакторную аутентификацию там, где это возможно.

подтверждение действий пользователя по электронной почте или СМС

4

МЕНЯЙТЕ пароли минимум раз в три месяца, не используйте их повторно.

5

НЕ СОХРАНЯЙТЕ пароли в программах или браузере.

6

НЕ ПЕРЕДАВАЙТЕ логины и пароли от своих учетных записей в информационных системах ОАО «РЖД» третьим лицам, в том числе — другим работникам компании.

7

НЕ ХРАНИТЕ пароли в электронной почте, а также на бумажных носителях на столе, под клавиатурой и в других общедоступных местах.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ