БЕЗОПАСНОСТЬ ПРИ РАБОТЕ С ЦИФРОВЫМИ ТЕХНОЛОГИЯМИ

Используйте средства удаленного доступа, разрешенные в ОАО «РЖД»

Проверяйте любые скачиваемые файлы средствами антивирусной защиты

При самостоятельной настройке необходимо использовать инструкции, предоставленные ОАО «РЖД»

Не открывайте лже-сайты, подозрительные вложения и почтовые рассылки, в отношении которых у вас есть сомнения

На устройствах, с которых организован удаленный доступ, используйте лицензионные средства Антивирусной защиты

Используйте надежные пароли на своих устройствах (роутеры, ПК, и др.), не менее 8 символов со строчными и прописными буквами, другими символами

ВАЖНО:

1. **Никому не сообщайте свои пароли!** Сотрудники ИТ-поддержки не спрашивают ваши логины или пароли для решения инцидентов
2. Сотрудники банков никогда не должны спрашивать реквизиты ваших банковских карт, персональные данные или пароли
3. При подозрении на компрометацию ваших паролей или утечке важной информации незамедлительно обращайтесь в службу поддержки.

ПОЛЕЗНАЯ ИНФОРМАЦИЯ

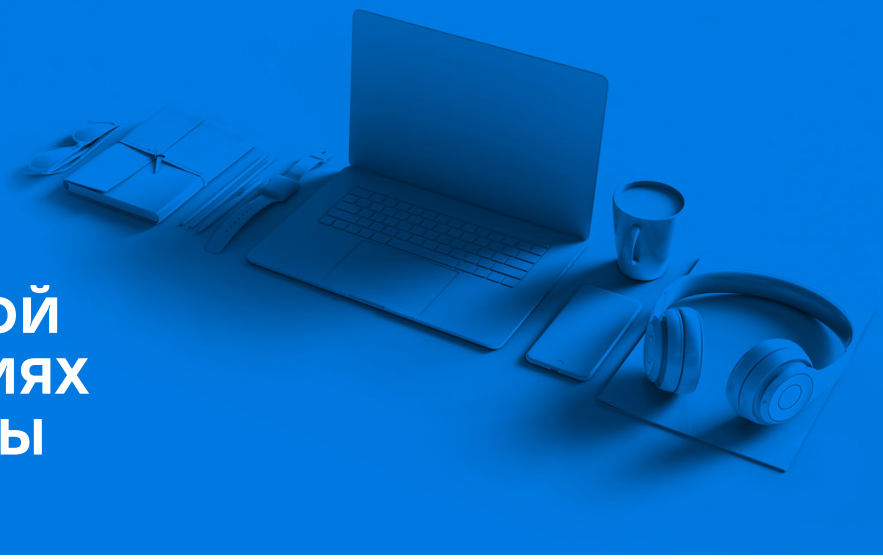
Правила безопасной работы из дома

Обучающий курс о том, как безопасно адаптироваться к удаленной работе

Наведите камеру смартфона на QR-код для открытия WEB страницы

СОВЕТЫ ОТ ВЕДУЩИХ РОССИЙСКИЙ КОМПАНИЙ ПО БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ ПРЕДСТАВЛЕНЫ НА СЛЕДУЮЩИХ СЛАЙДАХ

GROUP IB



ПРАВИЛА ЦИФРОВОЙ ГИГИЕНЫ В УСЛОВИЯХ УДАЛЕННОЙ РАБОТЫ

НАСТРОЙКА УДАЛЕННОГО ДОСТУПА

Заранее позаботьтесь о получении удаленного доступа к необходимым ресурсам и следуйте указаниям IT-специалистов для его настройки.

ЛИЧНОЕ И РАБОЧЕЕ

По возможности работайте на корпоративном компьютере. Не загружайте и не открывайте корпоративные файлы на личных устройствах.

РАЗРЕШЕННЫЕ КАНАЛЫ СВЯЗИ

Если использование определенных мессенджеров ранее не было разрешено корпоративным регламентом, не начинайте их использование сейчас.

БДИТЕЛЬНОСТЬ

Домашняя сеть не защищается отделом ИБ, поэтому будьте внимательны — атакующие могут воспользоваться ситуацией и направить усилия на менее защищённых пользователей.

ДВУХФАКТОРНАЯ АУТЕНТИФИКАЦИЯ

Проверьте, настроена ли двухфакторная аутентификация в почте, в мессенджерах и при VPN подключении.

ПРОВЕРКА СВЯЗИ С IT

Убедитесь, что вы точно знаете, как и по какому каналу можно быстро связаться с IT-специалистами при возникновении проблем.

ПАРОЛЬ ДЛЯ РОУТЕРА

Обязательно смените стандартный пароль домашнего роутера, иначе злоумышленники легко смогут получить доступ к вашим данным.

ДРУГИЕ ПОЛЬЗОВАТЕЛИ

Объясните близким, что вашим рабочим компьютером пользоваться нельзя, чтобы избежать случайного заражения устройства или потери данных.

education@group-ib.com
group-ib.ru/cyber-education

GROUP IB

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Защита и поддержание непрерывности бизнеса в эпоху перемен

Подразумевается, что, работая из дома, сотрудники соблюдают те же стандартные правила кибербезопасности, что и в офисе. Но использование личных ноутбуков и домашних сетей сопряжено с гораздо более серьезными рисками, чем работа в защищенной корпоративной сети. Кроме того, значительно возрастает нагрузка на IT-отделы.

Осведомленность о принципах IT-безопасности сейчас важна, как никогда прежде

В какой бы сфере ни работала компания и какого бы размера она ни была, проблемы с кибербезопасностью часто возникают из-за неправильного использования IT-ресурсов сотрудниками, а также заражения принадлежащих компании устройств. Это означает, что в большинстве случаев компании могут снизить риск утечки данных, повысив осведомленность своих сотрудников о безопасном обращении с IT-ресурсами.

Неправильное использование сотрудниками IT-ресурсов затронуло 52% корпораций и 50% предприятий малого и среднего бизнеса

Заражение корпоративных устройств вредоносными программами имело место в 51% корпораций и 49% предприятий малого и среднего бизнеса

Инциденты, вызванные несанкционированным мобильным обменом данными, случались в 48% корпораций и 43% предприятий малого и среднего бизнеса

Заражение личных устройств вредоносным ПО происходило в 48% корпораций и 47% предприятий малого и среднего бизнеса

Подобное поведение и инциденты такого рода могут обойтись бизнесу очень дорого.

Средний финансовый ущерб от утечки данных, вызванной нецелевым использованием IT-ресурсов сотрудниками, составляет 116 000 $ для малого и среднего бизнеса и 1 195 000 $ для корпораций.

Вне зависимости от масштаба бизнеса нарушения кибербезопасности всегда влекут за собой различные финансовые убытки: штрафы и санкции, рост страховых выплат, необходимость приобретения нового ПО, рост расходов на PR и обучение и т. д.

Например, в 2019 г. средние затраты корпораций в связи с утечками данных составили в числе прочего 182 000 $ на обновление инфраструктуры, 140 000 $ на обучение персонала и 161 000 $ на дополнительные PR-активности.

Источник всех указанных здесь данных – отчет IT Security Economics 2019.

«Одна из самых актуальных зафиксированных нами спам-кампаний имитирует рассылки от Всемирной организации здравоохранения. Здесь злоумышленники делают ставку на доверие к ВОЗ, которая играет важную роль в предоставлении достоверной информации о коронавирусе».

Константин Игнатьев
руководитель группы анализа веб-контента «Лаборатории Касперского»

Реагирование на актуальные угрозы

Любому бизнесу следует серьезно задуматься о снижении риска утечки данных – и важную роль в этом могут сыграть тренинги для повышения осведомленности в области кибербезопасности.

Руководители 33% корпораций и 27% предприятий малого и среднего бизнеса, столкнувшихся с инцидентами безопасности, заявили, что планируют увеличить вложения в обучение сотрудников во избежание повторения этих проблем. Проведение таких тренингов действительно должно стоять на первом месте среди прочих мер обеспечения кибербезопасности. Всегда лучше предотвратить инцидент, чем устранять его последствия.

Если вы задумываетесь о проведении тренингов для повышения осведомленности в области безопасности, сейчас самое время действовать. Все внимание в мире приковано к пандемии, и киберпреступники только и ждут благоприятного момента.

На конец января этого года «Лаборатория Касперского» обнаружила 32 различных вредоносных файла, распространяемых под видом информации о коронавирусной инфекции.

Не время медлить

Нельзя терять время. Начните просвещать своих сотрудников в вопросах кибербезопасности прямо сейчас, чтобы изменить их привычки и модель поведения и защитить свой бизнес

Памятка для сотрудников

Вот памятка, которую вы уже сейчас можете распространить среди сотрудников и IT-специалистов

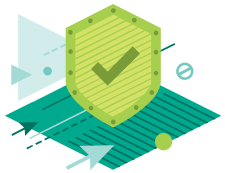
- ☑ Регулярно проводите обучение для повышения осведомленности о киберугрозах, чтобы сотрудники могли противостоять направленным на них атакам
- ☑ Проследите, чтобы на всех устройствах с доступом к корпоративным сетям и данным было установлено защитное решение, желательно под управлением корпоративного администратора.
- ☑ Проследите, чтобы все конфиденциальные данные на смартфонах, планшетах и ноутбуках хранились в зашифрованном виде.
- ☑ Обеспечьте защиту вашей домашней сети Wi-Fi! Смените пароль и настройте гостевую сеть для друзей и гостей, бывающих в вашем доме. Используйте максимально высокий уровень шифрования.
- ☑ Задействуйте двухфакторную аутентификацию.
- ☑ Используйте VPN.
- ☑ Будьте бдительны: остерегайтесь фишинговых писем и сайтов.
- ☑ Если вы работаете с личного устройства, удостоверьтесь, что на нем установлены сетевой экран и антивирусное ПО последних версий. Обновите приложения и операционные системы.
- ☑ Не используйте свою личную почту для рабочей переписки. Для обмена документами и другими данными используйте корпоративные ресурсы.

Советы по обеспечению непрерывности бизнеса

- ☑ Начните с базовых правил, которые помогут снизить риск возникновения инцидентов кибербезопасности.
- ☑ Привейте всем сотрудникам необходимые навыки в сфере кибербезопасности. Мы рекомендуем воспользоваться нашим тренингом Kaspersky Automated Security Awareness Platform. Подготовка и запуск программы потребуют от вас не больше 10 минут, а ваши сотрудники получат важные навыки и смогут применить их на практике уже после первого занятия.
- ☑ Снабдите IT-специалистов общего профиля практическими навыками для распознавания возможных атак и сбора данных об инцидентах, воспользовавшись нашим онлайн-курсом по кибербезопасности для IT-специалистов (CITO).
- ☑ Защитите репутацию компании в кризисной ситуации, в том числе разработайте и примените меры на случай инцидента IT-безопасности. Kaspersky Incident Communication – тренинг, который научит руководителей высшего звена и специалистов по информационной безопасности и корпоративным коммуникациям эффективно сотрудничать в случае инцидента.

Пробная версия Kaspersky ASAP: k-asap.com/ru
Kaspersky Security Awareness: www.kaspersky.ru/awareness

www.kaspersky.com



ИСПОЛЬЗУЙТЕ ЛИЦЕНЗИОННОЕ АНТИВИРУСНОЕ ПО и вовремя обновляйте антивирусные базы на всех устройствах

Регулярно **ОСУЩЕСТВЛЯЙТЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ** данных на всех устройствах

Регулярно **УСТАНАВЛИВАЙТЕ ОБНОВЛЕНИЯ СТОРОННЕГО ПО** на всех устройствах

Регулярно **МЕНЯЙТЕ ПАРОЛИ** на всех устройствах; пароли должны содержать не менее 8-12 символов, строчные и прописные буквы, цифры и другие знаки

ПРОВЕРЯЙТЕ ВСЕ ФАЙЛЫ из входящей электронной почты и социальных сетей на вирусы перед тем, как открыть их

НЕ ОТКРЫВАЙТЕ ПОДОЗРИТЕЛЬНЫЕ ВЛОЖЕНИЯ в электронной почте и социальных сетях, особенно если это архивы или исполняемые файлы (.exe)

Обязательно **ПРОВЕРЯЙТЕ НА ВИРУСЫ ЛЮБОЙ НОСИТЕЛЬ** при подключении к ПК

МИНИМИЗИРУЙТЕ РАБОТУ С ВНЕШНИМИ ИСТОЧНИКАМИ ИНФОРМАЦИИ на компьютере, где установлен банк-клиент

ВЫНИМАЙТЕ СРЕДСТВА АУТЕНТИФИКАЦИИ из портов ПК по завершении работы с банк-клиентом

НЕ ПРОВОДИТЕ ФИНАНСОВЫЕ ТРАНЗАКЦИИ в публичных местах с бесплатным беспроводным интернет-доступом (Wi-Fi)

По возможности **ИСПОЛЬЗУЙТЕ SMS-АУТЕНТИФИКАЦИЮ** при совершении любых онлайн-платежей

Никогда **НЕ ПЛАТИТЕ ЗЛОУМЫШЛЕННИКАМ ВЫКУП** в случае блокировки компьютера или данных