ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ НА РАБОЧЕМ МЕСТЕ

Основные правила для безопасной работы с данными и устройствами

Блокировка и выключение устройств

Блокируйте компьютер при каждом уходе с рабочего места, для этого используйте сочетание клавиш Win + L, если вы используете Windows и Command + Control + Q, если вы используете macOS.
Выключайте устройства, если они не будут использоваться длительное время. Это защитит данные на компьютере от несанкционированного доступа.

Безопасность USB-устройств и жестких дисков

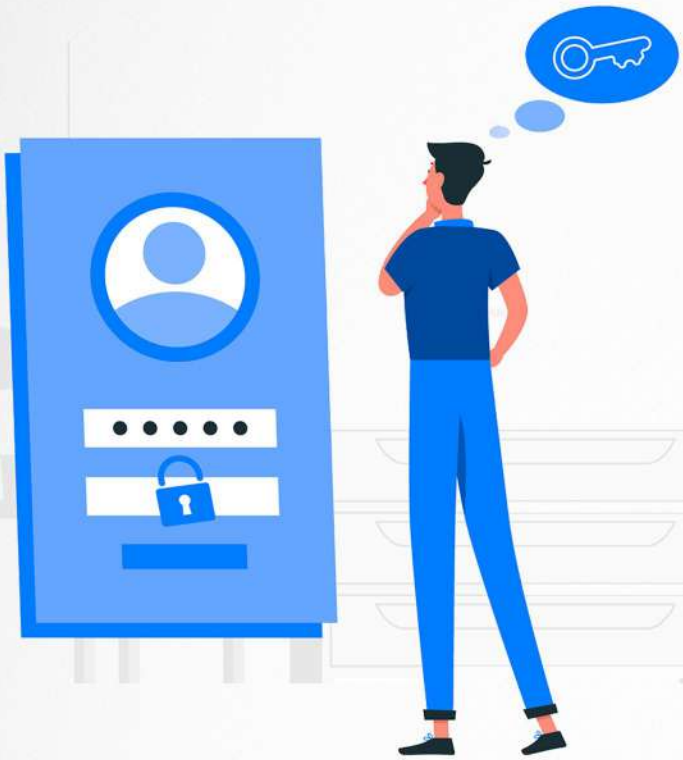
Используйте только те USB-устройства, в чьей безопасности вы уверены. Не подключайте случайно найденные или полученные от незнакомцев носители.
Храните ваши USB-устройства и жесткие диски в надежных местах и не передавайте их посторонним, даже коллегам.

Политика чистого стола

Убирайте рабочий стол в конце рабочего дня. Не оставляйте на нем документы и бумаги, содержащие конфиденциальную информацию, физические носители информации (флешки, жесткие диски и т.д).
Храните документы в защищённых шкафах, сейфах или других защищенных местах.

Базовые правила работы с конфиденциальной информацией

Не делитесь конфиденциальной информацией без необходимости, даже в разговоре.
Любая рабочая информация, попадающая к вам в руки является конфиденциальной, на них необязательно будут стоять пометки «Конфиденциально», «Не для печати», «Особое обращение» и т.п.



Парольная политика

Никому не сообщайте пароли для входа. Коллеги и родственники не исключение, они могут навредить даже без злого умысла.
Вместо простых паролей, например «petr27.02», устанавливайте сложные пароли, которые:
- содержат большие и маленькие буквы,
- содержат цифры и символы,
- состоят минимум из 12 символов.

Пароль должен легко запоминаться. Лучший вариант - парольная фраза, можно вводить русские выражения на английской раскладке клавиатуры.
Пример: "fkkj?Ufkjxrf!" (Алло, Галочка!).
Не используйте распространенные выражения, такие как «мойпароль».

Регулярно меняйте пароли и не используйте одинаковые пароли для разных аккаунтов.

Базовые правила работы с персональными данными

Персональными данными могут быть ФИО, адреса, телефоны и адреса электронных почт. Одним словом, персональные данные - это любая информация относящаяся прямо или косвенно к физическому лицу.

Минимизируйте сбор и хранение персональных данных, используйте их только по необходимости. Хранить персональные данные нужно бережно, на компьютерах и других рабочих устройствах они должны быть зашифрованы.

Облачные хранилища

Используйте только корпоративные сервисы для хранения рабочих данных. Не храните конфиденциальные или личные данные в облачных сервисах, не предназначенных для этого.
Регулярно совершайте резервное копирование, это снизит риск полной утраты данных.

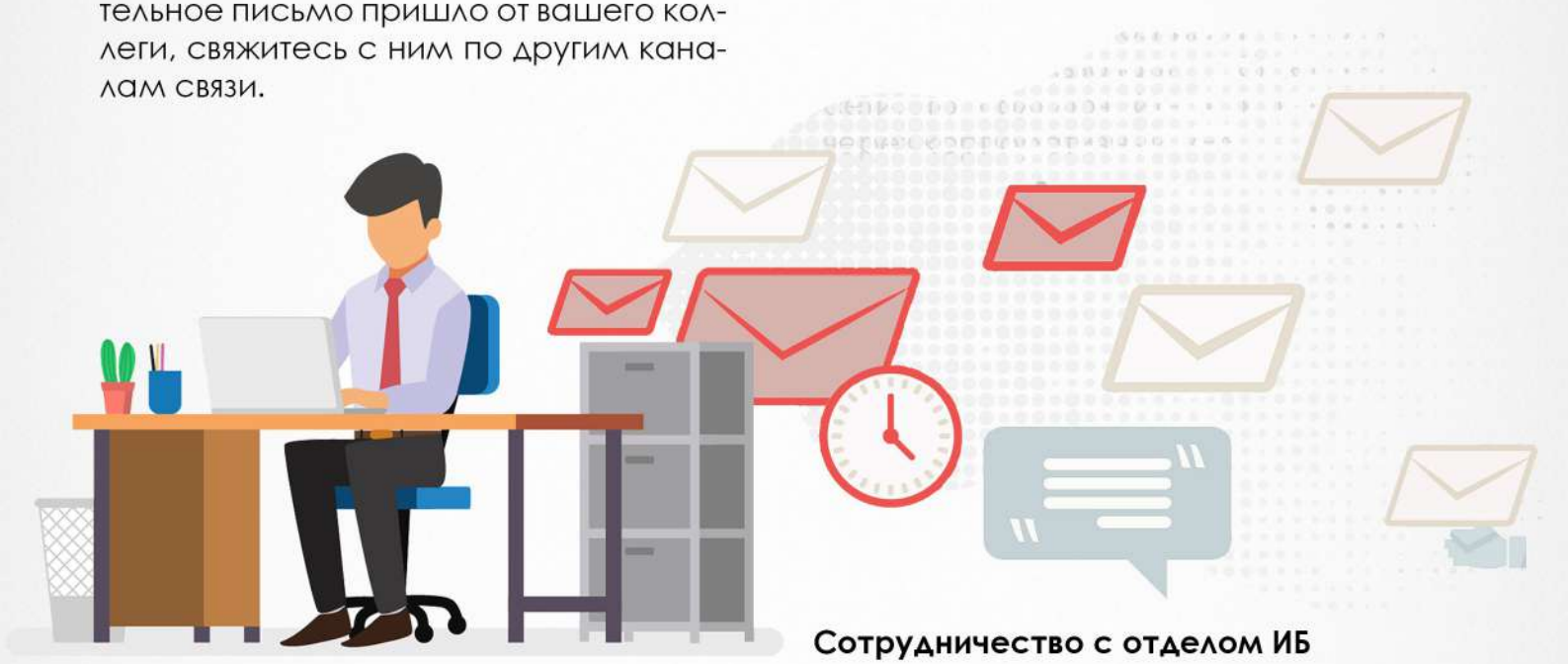
Разграничение личной и рабочей почты

Используйте разные почтовые аккаунты для личных и рабочих переписок, чтобы избежать случайной утечки данных.
Не открывайте рабочую почту в публичных или ненадёжных Wi-Fi сетях.

Подозрительные письма в электронной почте

Не открывайте письма от неизвестных отправителей или с подозрительными ссылками. Вот некоторые действия, которые помогут вам распознать мошенническое письмо:

• Проверьте, соответствует ли адрес отправителя официальному домену компании, если вам пришло внутреннее письмо. Домен может включать в себя похожие символы, например, *evseev@k0mpania.ru* вместо похожего *evseev@kompania.ru*. Если подозрительное письмо пришло от вашего коллеги, свяжитесь с ним по другим каналам связи.



• Просмотрите текст письма на предмет грамматических или орфографических ошибок, они могут указывать на мошенническую рассылку.

• Будьте осторожны, если письмо предлагает загрузить файл или перейти по ссылке, особенно от неизвестного отправителя. Никогда не вводите данные на сайтах при переходе по ссылке из письма, лучше найдите нужный раздел на официальном сайте сами.

Подключение и работа через Wi-Fi

Подключайтесь во время работы только к защищённым сетям Wi-Fi, предоставленных вашей организацией, для этого уточните наименование Wi-Fi точки доступа у сотрудников технической поддержки.

Не подключайтесь к Wi-Fi точкам доступа которые предоставляют доступ в Интернет без пароля. Например, если во время командировки возникла необходимость использовать общественные сети, то подключайтесь к ней только через корпоративный VPN.

Сотрудничество с отделом ИБ

Незамедлительно сообщайте в подразделение информационной безопасности с пометкой «инцидент ИБ» о всех случаях, связанных с информационной безопасностью, включая неправомерное присутствие посторонних лиц в офисе, получение фишинговых писем или обнаружение подозрительных ссылок.

С пожеланиями безопасности, StopPhish