Битрикс24

Полезные привычки, которые мы рекомендуем соблюдать не только в рабочее время...

Цифровая гигиена должна быть такой же естественной для каждого сотрудника, как и личная. Мы не будем называть ее корпоративной, так как она не должна прекращаться даже после работы.

Авторизация

- **Использовать надежный и уникальный пароль**
  Он нужен не только в Битрикс24. Например, взлом электронной почты может привести к доступу к другим сервисам: злоумышленник может запросить сброс пароля и получить доступ к другим аккаунтам, а также к конфиденциальной информации.
- **Не записывать пароли и не сообщать другим**
  использовать менеджер паролей для безопасного хранения и управления.
- **Настраивать двухфакторную аутентификацию во всех сервисах, где это возможно**
  это добавит дополнительный уровень защиты аккаунтов.
  Не забыть сохранить резервные коды.
- **Регулярно обновлять пароли**
  не менее 4х раз в год. Это снижает риск взлома, так как старые пароли могут быть скомпрометированы.

ПК и смартфон

- **Не оставлять гаджеты без присмотра**
  блокировать компьютер и телефон с помощью пароля или PIN-кода при уходе. Например, на ПК блокировать сочетанием клавиш Win+L или Ctrl+Alt+Del -> «Заблокировать».
- **Настроить время блокировки экрана**
  подобрать минимальный период времени, после которого включается блокировка экрана.
- **Не скачивать и не использовать нелицензионное ПО**
  это поможет избежать вирусов и других угроз безопасности.
- **Регулярно обновлять**
  приложения, веб-браузеры, операционные системы и прошивки до последних версий для устранения или исправления возможных уязвимостей безопасности.
- **Проверять источники приложений и файлов**
  загружать только из официальных магазинов и проверять файлы на вирусы перед их открытием.
- **Обязательно проверять все разрешения, предоставляемых установленным приложениям**
  некоторые приложения могут запрашивать доступ к данным, которые им не нужны для работы. Если приложения автоматически обновляются с маркетплейсов, то рекомендуется регулярно проводить аудит предоставленных разрешений.
- **Удалять неиспользуемые приложения**
  это уменьшает количество потенциальных уязвимостей, освобождает место на устройстве и помогает улучшить производительность.
- **Использовать надежный антивирус**
  для ПК и мобильных устройств. Это поможет защитить данные и устройства от вредоносных программ.
- **Не подключать к ПК неизвестно откуда взявшиеся флешки**
  они могут содержать вирусы или другие вредоносные программы.
- **Перед утилизацией или продажей компьютера, планшета или смартфона, нужно сбросить систему**
  это предотвратит доступ к вашим личным данным новому владельцу устройства.
- **Покидая рабочее место, убирать документы и съемные носители информации**
  в места, недоступные посторонним лицам — в запираемые шкафы, ящики стола, сейфы.
- **Перед отправлением документа на печать проверять имя/местоположение принтера**
  распечатанные документы забирайте из принтера сразу после печати.
- **Уничтожать документы на бумажных носителях, не имеющие ценности, утратившие значение**
  например, с помощью шредера.

Почта, мессенджеры и соц. сети

- **Не переходить по подозрительным ссылкам, в которых вы не уверены**
  это может привести к заражению вашего устройства вирусами или к фишинговым атакам.
- **Не открывать письма, выглядящие подозрительно**
  они могут содержать вредоносные программы или фишинговые ссылки.
- **Не открывать письма, выглядящие подозрительно**
  они могут содержать вредоносные программы или фишинговые ссылки.

Что должно насторожить:

- **Вложенные файлы:** неизвестное расширение, двойное расширение или расширение исполняемых файлов (например, *exe, *.scr, *bat *.vbs и т.п.).
- **Ссылки в содержании письма:** при наведении курсора показывают другой адрес в левой нижней строке браузера.
- **Грамматические ошибки, опечатки, подмены:** замена буквы цифрами, например, «0» на «О».
- **Некачественная графика**
- **Обращения общего характера:** такие как «Уважаемый клиент», «Дорогой друг».
- **Срочные просьбы:** подтвердить ваш адрес или личные данные: «Срочно!», «Сегодня последний день!».
- **Угрозы и запугивания:** «у вас задолженность», «аккаунт будет удален».
- **Маскировка:** отправители маскируются под официальных представителей известных компаний, используя общие почтовые домены, такие как gmail.com, mail.ru и другие, вместо корпоративных адресов.
- **Подозрительные домены:** мошенники могут выдавать себя за крупную компанию, но их сайт будет иметь адрес, не связанный с названием.
- **Письма, выглядящие как ответные:** письма могут выглядеть как ответ на ваше предыдущее сообщение, но вы не отправляли никаких писем.

- **Не загружать подозрительные вложения**
  особенно из неожиданных писем и чатов.
- **Не переходить по объявлениям, обещающим «бесплатные» деньги, призы и скидки.**
  это часто является уловкой мошенников для получения ваших личных данных.
- **Использовать корпоративный мессенджер Битрикс24**
  рабочая переписка в мессенджерах и соцсетях создает угрозу для компаний. Мошенники могут получить доступ к этим переписками или написать от лица «руководителя». Это сложнее сделать, если в компании общаются внутри Битрикс24.

Конфиденциальность / личная информация

- **Не публиковать личную информацию**
  например, домашний адрес, номер телефона, номера кредитных карт.
- **Проанализировать и настроить приватность в социальных сетях**
  например, ограничить доступ к комментариям и просмотру фотографий.
- **Регулярно проверять историю активности аккаунтов.**
  следить за подозрительными действиями и своевременно реагировать на них.
- **Проводить все онлайн-транзакции на защищённых веб-сайтах**
  адреса которых начинаются с https:// и имеют значок замка слева от адресной строки.

Берегите свои данные
и будьте осторожны в сети!