Приложение 1
к приказу № 360 от 26.10.2022 г.
заведующий МДОУ «Детский сад № 19»
_____ М.В.Скворцова

Инструкция по информационной безопасности на рабочих местах для сотрудников МДОУ «Детский сад № 19»

Доступ к корпоративным ресурсам и сервисам

1. Используйте только сложные пароли: они должны быть не менее 12 знаков длиной, не состоять из словарных слов, содержать спецсимволы и цифры. Если пароль простой, злоумышленник сможет подобрать его простым перебором.
2. Пароли должны быть уникальными: не используйте один и тот же пароль для всех рабочих ресурсов. Тем более — не используйте его же и в личных целях. Достаточно будет утечки из одного из сервисов, чтобы скомпрометировать их все.
3. Пароли должны быть секретными: не записывайте пароль на бумаге и не храните около рабочего места; не вписывайте их в файлы и не делитесь ими с коллегами. Иначе случайный посетитель офиса или уволившийся сотрудник сможет воспользоваться таким паролем во вред компании.
4. Если сервис позволяет включить двухфакторную аутентификацию, включите ее. Это не позволит злоумышленнику получить доступ к сервису даже в случае утечки пароля.

О важности персональных данных

5. Не выкидывайте бумаги с персональными данными в мусорную корзину. Если их нужно выкинуть, воспользуйтесь шредером. Злоумышленники нередко изучают выброшенные бумаги и могут наткнуться на них.
6. Не передавайте файлы с персональными данными по открытым каналам (например, через Google Docs по прямой ссылке или через публичные файлохранилища). Тот же Google индексирует документы в доступе по ссылке, так что на них может наткнуться посторонний.
7. Не делитесь персональными данными клиентов с коллегами, чьи рабочие функции не требуют такого доступа. Если такая практика обнаружится во время аудита, то компанию ждут неприятности от регуляторов, да и вероятность утечки возрастает.

О самых распространенных киберугрозах

8. Тщательно проверяйте ссылки в письмах, прежде чем по ним переходить. Убедительно выглядящее имя отправителя — не гарантия подлинности. Злоумышленники могут попробовать подсунуть фишинговую ссылку, особенно если им удастся захватить почту кого-то из ваших коллег.
9. Если вы распоряжаетесь бюджетами, то никогда не переводите деньги на неизвестные счета только на основании письма или сообщения в

мессенджере. Позвоните человеку, якобы санкционировавшему перевод, или свяжитесь с ним по другому каналу и попросите устное подтверждение. Захватив почту или учетную запись в мессенджере, злоумышленник может легко подделать письменное «распоряжения начальника».

10. Не подключайте к рабочему компьютеру неизвестно откуда взявшиеся флешки. Атака через зараженный внешний накопитель — это не фантастика: злоумышленники действительно могут подбросить устройство в офис.
11. Не открывайте и не запускайте исполняемые файлы из непроверенного источника (например, присланные по почте). При открытии файла всегда нужно смотреть, не является ли он исполняемым (злоумышленники часто маскируют вредоносные файлы под офисные документы).

Базовые требования соблюдения информационной безопасности на рабочих местах

Подготовлено с использованием материалов сайта компании «Лаборатория Касперского»

Доступ к ресурсам и сервисам, обеспечивающим функции образовательной организации

1. **Используйте только сложные пароли:** они должны быть не менее 12 знаков длиной, не состоять из словарных слов, содержать спецсимволы и цифры. Если пароль простой, злоумышленник удаленно с помощью специальных программ сможет подобрать его простым перебором.
2. **Пароли должны быть уникальными:** не используйте один и тот же пароль для всех рабочих ресурсов. Тем более — не используйте его же и в личных целях. Достаточно будет утечки из одного из сервисов, чтобы скомпрометировать в этом случае доступ ко всем ресурсам.
3. **Пароли должны быть секретными:** не записывайте пароль на бумаге и не храните около рабочего места; не вписывайте их в файлы и не делитесь ими с коллегами. Иначе случайный посетитель или уволившийся сотрудник сможет воспользоваться таким паролем.
4. **Если сервис позволяет включить двухфакторную аутентификацию, включите ее.** Это не позволит злоумышленнику получить доступ к сервису даже в случае утечки пароля.

О важности персональных данных

1. **Не передавайте файлы с персональными данными по электронной почте или по открытым каналам** (например, через Google Docs по прямой ссылке или через публичные файлохранилища).
2. **Не делитесь персональными данными, к которым Вы по своим обязанностям имеете доступ,** с коллегами, чьи рабочие функции не требуют такого доступа, с посторонними лицами, с обучающимися.

О самых распространенных киберугрозах

1. **Тщательно проверяйте ссылки в письмах, прежде чем по ним переходить.** Убедительно выглядящее имя отправителя — не гарантия подлинности. Злоумышленники могут попробовать подсунуть фишинговую ссылку, особенно если им удастся захватить почту кого-то из ваших коллег.

2. **Убедитесь, что на всех рабочих компьютерах подключена автоматическая проверка антивирусом при подключении USB устройств** (флеш-накопители, карты памяти, переносные жесткие диски, телефоны сотрудников через USB) . При настройке антивируса установите отключение автозапуска любой информации с подключаемых через USB устройств. Не подключайте к рабочему компьютеру любые сторонние флеш носители.
3. **Не открывайте и не запускайте любые файлы из непроверенного источника** (например, присланные по почте). При открытии файла всегда нужно смотреть, не является ли он исполняемым (злоумышленники часто маскируют вредоносные файлы под офисные документы). Любой присланный по почте файл необходимо сначала сохранить в папку, выделенную на локальном компьютере для файлов, которые не проверены антивирусом, затем, не открывая его, запустить проверку на вирусы в этом файле.