муниципальное образовательное учреждение дополнительного образования Детский экологический центр «Родник»

наименование организации

Номер документа	Дата
01-02/98	17.06.2024

г. Ярославль

ПРИКАЗ

Об обеспечении информационной безопасности
при работе с электронной почтой и ведении сайтов
МОУ ДО ДЭЦ «Родник»

С целью обеспечения устойчивого функционирования информационной инфраструктуры и предотвращения реализации угроз безопасности информации, связанных с фишингом в МОУ ДО ДЭЦ «Родник»,

ПРИКАЗЫВАЮ:

1. Сотрудникам МОУ ДО ДЭЦ «Родник» проверять адрес отправителя электронного письма, даже в случае совпадения имени отправителя с уже известным контактом.
2. Сотрудникам МОУ ДО ДЭЦ «Родник» проверять содержащиеся в электронном письме ссылки путем наведения курсора на ссылку, не нажимая на нее (адрес появится во всплывающем окне), даже если письмо получено от пользователя с электронной почты в домене @yarregion.ru.
3. Сотрудникам МОУ ДО ДЭЦ «Родник» осуществлять проверку всех поступающих на электронную почту вложений, в том числе полученных от известных контактов, с использованием средств антивирусной защиты (не открывая вложение).
4. Сообщать директору Киселевой А.В. о письмах, в которых содержатся призывы к действиям (например, «проинструктировать», «открыть», «прочитать», «ознакомиться», «дать ответ»), с темами про финансы, банки, геополитическую обстановку или угрозы, письма на иностранном языке, с большим количеством получателей и орфографическими ошибками, а также, содержащие подозрительные ссылки и вложения.
5. Секретарю Сидоровой Е.В. отправлять на электронный адрес: ib@yarregion.ru для проверки письма, в которых содержатся призывы к действиям (например, «проинструктировать», «открыть», «прочитать», «ознакомиться», «дать ответ»), с темами про финансы, банки, геополитическую обстановку или угрозы, письма на иностранном языке, с большим количеством получателей и орфографическими ошибками, а также содержащие подозрительные ссылки и вложения.
6. Утвердить базовые требования соблюдения информационной безопасности на рабочих местах МОУ ДО ДЭЦ «Родник» (Приложение).
7. Секретарю Сидоровой Е.В. ознакомить сотрудников МОУ ДО ДЭЦ «Родник» с приказом под роспись.
8. Контроль за исполнением приказа оставляю за собой.

Директор МОУ ДО ДЭЦ «Родник» А.В. Киселева

Муниципальное образовательное учреждение дополнительного образования
Детский экологический центр «Родник»
г. Ярославль

Приложение

Базовые требования соблюдения информационной безопасности на рабочих местах

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.