Уважаемые коллеги!

В связи с переводом на дистанционное освоение образовательных программ и рекомендациями о возможности перевода преподавателей и сотрудников на удаленную работу, Центр информационной безопасности Цифрового блока НИУ ВШЭ прогнозирует рост числа кибератак на компьютеры, оборудование и незащищенные домашние сети студентов, преподавателей и сотрудников НИУ ВШЭ, которые перешли на удаленный режим работы. В группе риска может оказаться персонал финансовых и ИТ-подразделений, а целью кибератак может стать кража денег или персональных данных студентов, преподавателей и сотрудников.

Поэтому предлагаем ознакомиться с перечнем простых правил, которые помогут избежать большинства инцидентов информационной безопасности:

      Обновите программное обеспечение на домашнем компьютере до актуальных в настоящий момент версий. Проводить обновление следует не реже одного раза в две  недели;

      Для преподавателей и сотрудников, у которых есть разрешение на подключение к внутренним ресурсам НИУ ВШЭ, рекомендуем использовать VPN согласно выданной при разрешении доступа инструкции. В настоящее время проводятся финальные испытания системы VPN с двухфакторной аутентификацией. Как только система будет введена в промышленную эксплуатацию, указанные пользователи получат на корпоративные почтовые ящики инструкции по ее использованию;

      На домашнем компьютере обязательно используйте антивирусное программное обеспечение с актуальными антивирусными базами;

      Также в настоящее время участились случаи спам-атак. Будьте бдительны и не совершайте необдуманных действий, при получении почтовых сообщений от незнакомых людей не переходите по ссылкам и не открывайте приложения к письму без проверки антивирусным средством;

      В случае обнаружения подозрительного объекта (файла) на компьютере, необходимо проверить его с помощью антивирусного средства или на ресурсе [https://www.virustotal.com](https://mail2.hse.ru/owa/redir.aspx?C=6yKc94f-BAOVKbya72V2xnDWiMHHpXZGA64_1gEldQ360LYGcdLXCA..&URL=https%3a%2f%2fwww.virustotal.com), предварительно загрузив данный объект на сайт;

      Периодически меняйте пароль от своей учетной записи в домене НИУ ВШЭ - не реже одного раза в три-четыре месяца.

Для учетных записей внутреннего домена @hse.ru cделать удаленно это можно следующими способами:

1.       на портале корпоративной почты [https://mail.hse.ru](https://mail2.hse.ru/owa/redir.aspx?C=AyWOIFooIuCbKE6Xlzq_HMFuQSYY3SNwtnmSbKIKxqz60LYGcdLXCA..&URL=https%3a%2f%2fmail.hse.ru) (Параметры -> Сменить пароль)

2.       на портале Единого личного кабинета [https://lk.hse.ru](https://mail2.hse.ru/owa/redir.aspx?C=uczz3tR0pNyy-w_VtGhVlBiVG2mPavYpZlkBEU_w-uT60LYGcdLXCA..&URL=https%3a%2f%2flk.hse.ru) (Безопасность и доступ -> Смена пароля). Данный функционал работает только для работников, подписавших Соглашение между участниками электронного взаимодействия;

      Сообщайте в техническую поддержку о подозрительных спам-сообщениях, активностях и других инцидентах информационной безопасности, связанных с информационно-телекоммуникационной инфраструктурой НИУ ВШЭ;

      Контакты технической поддержки ИТ НИУ ВШЭ:

  Городской номер телефона: +7 495 771-32-22;

  WhatsApp, Viber: +7 915 363-35-03;

  Внутренний номер из телефонной сети НИУ ВШЭ: 22222;

  Письмо из формы в Едином личном кабинете ([https://lk.hse.ru](https://mail2.hse.ru/owa/redir.aspx?C=uczz3tR0pNyy-w_VtGhVlBiVG2mPavYpZlkBEU_w-uT60LYGcdLXCA..&URL=https%3a%2f%2flk.hse.ru), вкладка «Поддержка», кнопка «Написать в техподдержку»);

  e-mail: [22222@hse.ru](https://mail2.hse.ru/owa/redir.aspx?C=46EWO4zwZBW8YWFXfxLmij7RfDZ9omp1zSvGqbHsggL60LYGcdLXCA..&URL=mailto%3a22222%40hse.ru)