

Обучение от разстояние в електронна среда: информация, практически съвети и правила за сигурност и безопасна работа

- Всички педагогически специалисти и ученици имат създадени Google акаунти и Google имейли в домейна на училището.

- Обучението от разстояние в електронна среда (ОРЕС) в СУ „Симон Боливар“, град Пловдив се осъществява чрез електронни платформи Google G Suite за образованието, Google classroom - <https://classroom.google.com>

- ОРЕС включва: дистанционни учебни часове, самоподготовка, текуща обратна връзка за резултатите от обучението и оценяване. Дистанционните учебни часове включват синхронен урок, при който обучаващият и обучаемите взаимодействат в реално време, едновременно, присъствено, чрез визуален контакт през Google класна стая чрез Google Meet.

- Учениците се присъединяват към Google класна стая

- Учениците имат задължението да не разпространяват в различни социални мрежи предоставените от учителя/педагогическия специалист файлове, линкове или хипервръзки към материали, публикувани в Google класна стая, както и да не предоставят достъп на други лица до своите работи по заданията, публикувани в Google класна стая, извън домейна на училището.

- Учениците имат задължението да не предоставят и/или споделят с трети лица информация за потребителските си имена и персоналните си пароли за достъп до внедрената облачната платформа.

- Учителите/педагогическите специалисти имат задължението да не разпространяват в различни социални мрежи документи, файлове, линкове или хипервръзки към материали, публикувани в Google класна стая, както и да не предоставят достъп на други лица до работите на учениците по заданията, публикувани в Google класна стая, извън домейна на училището.

- Учителите/педагогическите специалисти/работниците и служителите имат задължението да не предоставят и/или споделят с трети лица информация за потребителските си имена и персоналните си пароли.

Ето няколко съвета и най-добри практики за киберсигурност за хора, работещи отдалечено:

1. Използвайте Мениджър на пароли

Мениджърът на пароли е чудесен начин да защитите всички онлайн акаунти и пароли. LastPass и 1Password са две от най-популярните системи за управление и за съхранение на криптирани пароли онлайн. Те дават възможност за сигурно споделяне на пароли и могат да се използват и за генерирането им, така че всички да имат лесен и безопасен достъп до всичко, което им е необходимо, за да си свършат работата.

2. Спазвайте физическа безопасност на своите устройства

Честа причина за нарушаване на сигурността е сценарий, при който се губи устройство (устройства). Независимо дали сте у дома, в друго помещение извън училище или на път, е задължително да разберете, че киберпрестъпниците са опортюнисти и ще се възползват от всеки шанс. Това означава, че защитата на всички устройства, използвани за достъп до всякакви работни данни, е от решаващо значение. Някои от най-добрите съвети включват:

- Използвайте защита с парола и заключване на екраните, като се използва най-сигурният метод, наличен за всяко устройство;
- Никога не изпускате устройствата си от поглед;

- Не позволявайте на никой друг да използва вашето устройство или да включва нещо в него, например USB;
- Инсталирайте софтуер за проследяване или опции „Find My Device“ за всяко устройство;
- Винаги архивирайте вашите файлове;
- Шифровайте чувствителните данни.

3. Избягвайте обществени или несигурни Wi-Fi мрежи

Изкушаващо е да се ползва достъп до безплатен Wi-Fi в различни обекти и пространства. Това обаче може да бъде много рисковано, тъй като несигурният трафик, включително чувствителна информация и идентификационни данни за влизане, може лесно да бъдат прихванати от хакер. Несигурните Wi-Fi мрежи могат да се използват и за разпространение на зловреден софтуер или за подправяне на обществена Wi-Fi мрежа за привличане на потребители и компрометиране на техните данни, без те да знаят. За да гарантирате своята сигурност, препоръчително е да избягвате такива обществени мрежи, когато е възможно.

4. Актуализирайте софтуера на всички устройства до последна версия

Кибер атакуващите постоянно търсят нови уязвимости в софтуера, който вашите устройства използват. Когато открият уязвимости, те използват специални програми, за да ги експлоатират и да хакнат устройствата, които използвате. Междувременно компаниите, създали софтуера за тези устройства, се стараят да ги поправят, пускайки актуализации. Като гарантирате, че вашите компютри и мобилни устройства инсталират тези актуализации незабавно, вие правите много по-трудно някой да ви хакне. За да поддържате софтуера, просто активирайте автоматично актуализиране, когато е възможно. Това правило важи за почти всяка технология, свързана към мрежа.