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

- ОУ „Екзарх Антим I“, град Пловдив разполага със собствен домейн, в който е внедрена облачната платформа G Suite for Education.
- Домейнът на училището се администрира от Биляна Вълева, на длъжност “Заместник-директор по учебната дейност”, която: управлява достъпа до информация за всички потребители на домейна на училището; създава и управлява индивидуални профили на ученици, педагогически специалисти, работници и служители в ОУ “Екзарх Антим I”, гр. Пловдив; ограничава и/или премахва профили на ученици, педагогически специалисти, работници и служители, които вече не са част от общността на ОУ “Екзарх Антим I”, гр. Пловдив и/или по други причини отсъстват за дълъг период от време; управлява достъпа до приложенията и функционалностите в тях за потребителите; настройва инструментите на G Suit for Education: Google Classroom, GMail, Google Диск, Google Документи, Google Таблици, Google Презентации, Google Формуляри и др. за нуждите за учене, преподаване и администриране в администрата конзола; оказва технологична и техническа подкрепа на педагогически специалисти, работници и служители в ОУ “Екзарх Антим I”, гр. Пловдив, както и на ученици и родители, за използване на инструментите на G Suit for Education за нуждите за учене, преподаване и администриране;
- Всички документи, информации и други подобни, намиращи се в домейна на училището, са собственост на ОУ „Екзарх Антим I“, град Пловдив.
- Всички педагогически специалисти, работници, служители и ученици имат създадени Google акаунти и Google имейли в домейна на училището.
- Обучението от разстояние в електронна среда (ОРЕС) в ОУ „Екзарх Антим I“, град Пловдив се осъществява единствено и само чрез облачната платформа G Suite for Education и нейните инструменти.
- 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 чрез Google имейлите в домейна на училището: …@ekzarhantim1.com. Имейли, извън домейна на училището, не могат да се присъединят 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, в който е внедрена облачната платформа G Suite for Education.
- 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 G Suite for Education в домейна на училището по никакъв повод и при никакво обстоятелство.
- Учениците имат задължението да не използват персоналните си пароли за достъп до внедрената облачната платформа G Suite for Education в домейна на училището за достъп до други социални мрежи и приложения, използвани за лични нужди.

- 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, в който е внедрена облачната платформа G Suite for Education.
- 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 за достъп до внедрената облачната платформа G Suite for Education в домейна на училището, по никакъв повод и при никакво обстоятелство.
- Учителите/педагогическите специалисти/работниците и служителите имат задължението да не използват персоналните си пароли за достъп до внедрената облачната платформа G Suite for Education в домейна на училището за достъп до други социални мрежи и приложения, използвани за лични нужди.
- Родителите 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, в който е внедрена облачната платформа G Suite for Education.
- Родителите имат задължението да не предоставят и/или споделят с трети лица информация за потребителските имена на учениците и персоналните им пароли за достъп до внедрената облачната платформа G Suite for Education в домейна на училището, по никакъв повод и при никакво обстоятелство.
- Родителите имат задължението да не използват потребителските имена на учениците и персоналните им пароли за достъп до внедрената облачната платформа G Suite for Education в домейна на училището за достъп до други социални мрежи и приложения, използвани за лични нужди.

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

(адаптирано от https://www.govcert.bg/BG/NAW/Pages/%D0%A1%D1%8A%D0%B2%D0%B5%D1%82%D0%B8-%D0%B7%D0%B0-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D1%81%D0%B8%D0%B3%D1%83%D1%80%D0%BD%D0%BE%D1%81%D1%82-%D0%B8-%D0%BD%D0%B0%D0%B9-%D0%B4%D0%BE%D0%B1%D1%80%D0%B8-%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D0%B8,-%D0%BD%D0%B0%D1%81%D0%BE%D1%87%D0%B5%D0%BD%D0%B8-%D0%BA%D1%8A%D0%BC-%D1%85%D0%BE%D1%80%D0%B0%D1%82%D0%B0,--%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B5%D1%89%D0%B8-%D0%BE%D1%82%D0%B4%D0%B0%D0%BB%D0%B5%D1%87%D0%B5%D0%BD%D0%BE.aspx):

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 изпускайте 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.

5. И още …

- Не използвайте лични имейл адреси за работа и обучение;
- Не използвайте непроверени приложения за онлайн съобщения или друг софтуер, който може да представлява риск за сигурността;

Съвети за повишаване на сигурността ви онлайн:

https://safety.google/intl/bg/security/security-tips/

Интернет в ежедневието ни:

https://www.youtube.com/watch?v=NxvbVaOGvTk

Правила за безопасна работа в интернет:

https://www.youtube.com/watch?v=nYi7vAzrR9o

10 съвета за безопасност в интернет:

https://www.youtube.com/watch?v=Q_QhIGOH7sk

Видео урок "Безопасно в интернет"

https://www.youtube.com/watch?v=_0Z6b3lYyrk