ИНСТРУКТАЖ

Във връзка с писмо на министерството на образованието и науката № 9105-421/08.12.2020 г. и във връзка с преминаването към обучение в електронна среда, както и във връзка с неправомерно използване на ученически акаунти и нарушаване дисциплината при обучение в електронна среда

I. Електронните профили от типа …@edu.mon.bg са персонални! Тези служебни акаунти ще бъдат активни, докато учителят преподава в системата на училищното образование, респективно докато ученикът посещава училище от I до XII клас. С тях поетапно ще бъдат интегрирани всички платформи и информационни системи, използвани в образователния процес, поради което правилното им разпространение и съхранение е от изключителна важност!

1. Всеки профил отговаря на точно определен потребител и всеки трябва да се отнася отговорно и да пази своите данни.

2. **Да не се предоставя информация за потребителски имена и пароли** на трети лица, както и в различни електронни платформи и социални мрежи.

3. Да не се публикуват кодове на класни стаи в незащитени групи и канали!

4. **В профила си всеки потребител следва да въведе информация, с чиято помощ да може сам бързо да смени компрометирана или забравена парола – алтернативен имейл и/или мобилен телефон.** Ако такава информация не е въведена, смяната на парола може да бъде извършена единствено от директора/администратора на училището.

5. При съмнение за кражба на потребителски профил или компрометиран профил, незабавно да се уведоми директора/администратора в училище. При съмнение за кражба на директорски/администраторски профил трябва незабавно да се поиска нулиране на паролата от електронната поща, посочена в НЕИСПУО.

II. На учениците и учителите следва да се обърне специално внимание на следните аспекти:

6. Паролите трябва да бъдат едновременно достатъчно дълги и достатъчно сложни, да бъдат съставени от различни знаци и символи. Паролите не трябва да бъдат думи, имена или нещо, което лесно може да бъде асоциирано с техните собственици. Освен това паролите се „износват“, т.е. остаряват. Всяко едно въвеждане на парола за достъп от клавиатурата или екрана на дадено устройство предполага компрометирането на тази парола. Паролите трябва да бъдат сменяни периодично.

Неправилното управление на пароли може да доведе до значителни рискове от кражба и необратима загуба на информация, изтичане на чувствителни данни, пробив в информационните системи.

7. Всички потребители и/или администратори **не трябва** да използват пароли за достъп до системи на МОН за свои лични нужди (например: паролата за достъп до една

от информационните системи на МОН трябва да бъде различна от тази за достъп до личния адрес на електронната поща на потребителя).

8. Паролите са строго персонални и по никакъв повод и при никакво обстоятелство не следва да бъдат споделяни с трети лица. Те се считат за строго секретна информация.

9. При никакви обстоятелства паролите не трябва да бъдат изпращани по електронна поща, да бъдат записвани на хартиен носител, комуникирани по телефон, факс или друг несигурен или лесен за разчитане формат или канал, както и при никакви обстоятелства не трябва да бъдат въвеждани в електронни анкети.

10. Паролите не трябва да бъдат записвани във файл на работна станция, сървър или мобилно устройство в некриптиран вид.

11. Трябва да се обърне сериозно внимание на атаките от тип социално инженерство, които напълно заобикалят всички предприети технически мерки за защита и използват уязвимостта на човешкия фактор. Социалният инженеринг е метод за неоторизирано придобиване на информационни ресурси и/или потребителски права без използване на технически средства. Социалното инженерство използва главно психологически методи, а именно склонността на човек да се доверява. Атаките от типа социално инженерство протичат на две нива: Физическо ниво са офиси, телефони, кошчета за боклук, служебна поща. На работното място социалният инженер може просто да влезе, представяйки се за лице по поддръжката, и да се сдобие с потребителско име и парола. Психологическият подход използва утвърдени методи за убеждаване: представяне за някой друг, конформизъм, позоваване на авторитетна фигура, разсейване на отговорността или просто дружелюбно отношение. Най-честият и лесен начин да се сдобие трето лице с потребителско име и парола е, като го получи директно от потребителя чрез различни методи на убеждаване, подвеждане, неволно споделяне, подвеждане с цел постигане на финансови облаги и пр. Социалното инженерство е предпочитан метод, с който да се започне атака върху дадена система, защото при невнимание от страна на потребителя атакуващият лесно може да получи необходимата информация.