Szkolenie

Cyberbezpieczeństwo dla nauczycieli: Jak chronić siebie i uczniów przed cyberzagrożeniami?

Strona szkolenia | Terminy szkolenia | Rejestracja na szkolenie | Promocje

Opis szkolenia

W dobie rosnących zagrożeń cyfrowych nauczyciele stają się jednym z głównych celów cyberprzestępców. Phishing, deepfake, ataki na urządzenia mobilne czy cyberstalking – to tylko niektóre z wyzwań, na które warto się przygotować.

Szkolenie dostarczy praktycznej wiedzy na temat ochrony prywatności w sieci, bezpiecznej pracy z uczniami oraz zabezpieczania danych. Omówimy również wpływ sztucznej inteligencji na cyberbezpieczeństwo oraz nauczymy, jak reagować w przypadku cyberataku.

Dowiedz się, jak skutecznie chronić siebie i uczniów w cyfrowym świecie!

Korzyści

- Nauczysz się rozpoznawać phising, deepfake oraz techniki stosowane przez cyberprzestępców.
- Dowiesz się, jak minimalizować swój ślad cyfrowy i zabezpieczyć konta w mediach społecznościowych.
- Poznasz zasady ochrony danych osobowych.
- Zrozumiesz zarówno zagrożenia, jak i możliwości wykorzystania sztucznej inteligencji w edukacji.
- Nauczysz się, jak reagować w przypadku utraty danych, włamania na konto czy kradzieży tożsamości.
- Zdobędziesz wiedzę o tworzeniu silnych haseł, bezpiecznym korzystaniu z komunikatorów i ochronie urządzeń mobilnych.

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.

Harmonogram szkolenia

Moduł 1: Nowoczesne zagrożenia cyfrowe – czyli jak dziś atakują hakerzy

- Phishing 2.0 – personalizowane ataki i deepfake phishing.
- Smishing i vishing – jak nie dać się oszukać botom przez telefon.
- Juice jacking – ataki na urządzenia mobilne.

Moduł 2: Ochrona prywatności w sieci – nauczyciel też jest celem

- Ślad cyfrowy – co to jest i co można znaleźć o Tobie online.
- Media społecznościowe – dobre praktyki prywatności.
- Cyberstalking i kradzież tożsamości – jak się chronić.

Moduł 3: Bezpieczna praca z uczniami – urządzenia, sieci i dane osobowe

- RODO w pigułce dla nauczycieli – co wolno, a czego nie?
- Jak bezpiecznie korzystać z komunikatorów?
- Ochrona danych uczniów i materiałów edukacyjnych.
- Dobre praktyki i jak tworzyć bezpieczne hasła.

Moduł 4: Sztuczna inteligencja a cyberbezpieczeństwo dziś i jutro

- AI jako narzędzie ataku – deepfake, automatyczny phishing oraz czym są boty?
- AI w edukacji – szanse i zagrożenia. Jak świadomie korzystać z AI w nauczaniu?
- Jak bezpiecznie korzystać z AI?

Moduł 5: Cyberatak – co robić, gdy się wydarzy?

- Odzyskiwanie danych i backupy – coś, co może uratować dane.
- Scenariusze incydentów – utrata danych, włam na konto bankowe, kradzież profilu czy szantaż.
- Zgłaszanie incydentów – komu, gdzie i jak.

Tagi:

Adres korespondencyjny:
DAGMA Szkolenia IT | ul. Bażantów 6a/3 | Katowice (40-668)
tel. 32 793 11 80 | szkolenia@dagma.pl
szkolenia.dagma.eu

DAGMA Sp. z o.o. z siedzibą w Katowicach (40-478), ul. Pszczyńska 15
Sąd Rejonowy Katowice-Wschód w Katowicach Wydział VIII Gospodarczy
KRS pod numerem 0000130206, kapitał zakładowy 75 000 zł
Numer NIP 634-012-60-68, numer REGON: 008173852
DAGMA Sp. z o.o. posiada status dużego przedsiębiorcy
w rozumieniu art. 4c ustawy o przeciwdziałaniu nadmiernym
opóźnieniom w transakcjach handlowych.