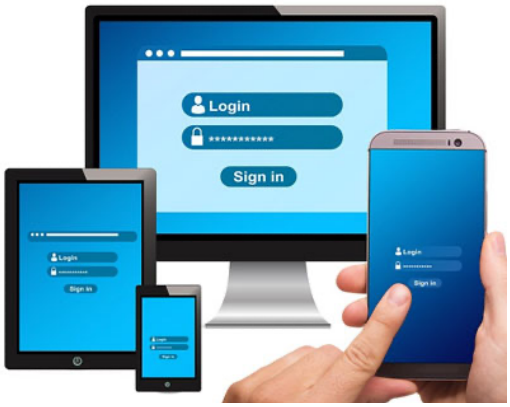
Wat is een goed wachtwoord?

Waarom is het belangrijk om veilige wachtwoorden te gebruiken en hoe ziet een veilig wachtwoord er eigenlijk uit?



Opdracht

Als je e-mails wilt schrijven, iets op een sociaal netwerk wilt posten of gewoon iets online wilt bestellen, moet je altijd inloggen met je eigen gebruikersnaam en wachtwoord. Voor elk e-mailaccount, elk sociaal netwerk en elke online winkel heb je je eigen wachtwoord nodig, en dat moet zo veilig mogelijk zijn!
Maar waarom is het belangrijk om veilige wachtwoorden te gebruiken en hoe ziet een veilig wachtwoord er eigenlijk uit?

Uitwerking

Als je e-mails wilt schrijven, iets op een sociaal netwerk wilt posten of gewoon iets online wilt bestellen, moet je altijd inloggen met je eigen gebruikersnaam en wachtwoord. Voor elk e-mailaccount, elk sociaal netwerk en elke online winkel heb je je eigen wachtwoord nodig, en dat moet zo veilig mogelijk zijn!
De meeste mensen gebruiken echter hetzelfde wachtwoord voor elke account en meestal een heel eenvoudig wachtwoord. Volgens een onderzoek van Nordpass (https://nordpass.com/most-common-passwords-list/), waren de tien meest gebruikte wachtwoorden wereldwijd in het afgelopen jaar:

1. 123456
2. 123456789
3. 12345
4. qwerty
5. wachtwoord

6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567
11. Waarom is het zo belangrijk om een veilig wachtwoord te hebben en wat kunnen de gevolgen zijn als iemand uw wachtwoord te weten komt, bv. voor sociale media, e-mail of online winkelen?
12. De meest voorkomende wachtwoorden in uw land staan ook vermeld op https://nordpass.com/most-common-passwords-list/.
    a) Wat waren de 10 meest voorkomende wachtwoorden in uw land?
    b) Waarom gebruikten mensen deze wachtwoorden?
13. De sterkte van een wachtwoord kan ook online worden gecontroleerd https://www.security.org/how-secure-is-my-password/
    a) Hoe lang heeft een computer nodig om de tien wachtwoorden uit 2 a) te kraken?
    b) Wat is een goed wachtwoord? Gebruik dit online hulpmiddel om de kenmerken te ontdekken en te beschrijven voor het maken van een goed wachtwoord dat bij u past en test uw criteria!

Oplossing
Naar punt 1)
Een gekraakt wachtwoord kan leiden tot identiteitsdiefstal op het internet. Dit heeft de volgende mogelijke gevolgen.
De dieven kunnen uit naam van de beroofde persoon communiceren op sociale media of via e-mail. Dit kan resulteren in reputatieschade (bv. beledigen van mensen of andere ongepaste posts) of zelfs criminele handelingen (dreigen met geweld, aankondigen van criminele handelingen).
Op het gebied van internetwinkelen kunnen de dieven op kosten van de bestolenen bestellen en zo financiële schade veroorzaken.
Naar punt 3)
a) Computers kraken bijna onmiddellijk alle wachtwoorden van punt 2.
b) De volgende criteria beïnvloeden de veiligheid van een wachtwoord
    a) De lengte van het wachtwoord
    b) Gebruikte tekensoorten (alleen cijfers, letters, speciale tekens)
    c) De manier waarop personages zijn samengesteld

In het algemeen is het moeilijk te beschrijven wanneer een wachtwoord veilig is
Om een voorbeeld te geven: het wachtwoord "11111111" zou onmiddellijk worden gekraakt, terwijl het wachtwoord "111111111111111111111" 83 quintiljoen jaar nodig heeft om te worden gekraakt.
Mogelijke kenmerken zijn
- 12 Karakters
- Gebruik cijfers, letters en speciale tekens

De veiligheid van een wachtwoord hangt ook af van persoonlijke factoren zoals mentale capaciteiten zoals retentiviteit, het vermogen om mnemotechnieken te gebruiken, maar ook van het niveau van beveiliging dat voor een wachtwoord nodig is.

Didactiek

Het onderwerp cyberveiligheid kan worden geïntegreerd in het techniekonderwijs aan het begin van het voortgezet onderwijs. Aangezien in ieder geval e-mailcommunicatie en het gebruik van sociale media begint in de onderbouw van het voortgezet onderwijs (gemiddeld tussen twaalf en dertien jaar) legt men bij de taak cyberveiligheid een verband met het persoonlijke leven van de leerling en moet men laten zien wat de gevolgen zijn van onzorgvuldige wachtwoordkeuze.

Taak twee en drie zijn bedoeld om de leerlingen het vermogen te laten ontwikkelen om optimale wachtwoorden te kiezen voor hun eigen gebruik. Het is belangrijk om in taak drie een reflectiefase te integreren waarin de eigen kenmerken voor een goed wachtwoord worden getest. Leerlingen moeten zelf een wachtwoord bedenken, de sterkte ervan testen en proberen het te onthouden en na deze fase hun kritiek te optimaliseren.
Het is belangrijk dat de leerkracht vermeldt dat er geen perfect wachtwoord bestaat en dat de keuze van een wachtwoord afhangt van persoonlijke factoren, zoals hierboven vermeld. Daarna moeten extra veiligheidsmaatregelen bij het gebruik van het web worden besproken: (beveiligde verbindingen gebruiken, geen marginale websites bezoeken, zie https://www.security.org/how-secure-is-my-password/ "andere manieren om uzelf online te beschermen")