Beveilig je geheimen

Wees realistisch over privacy en veiligheid

Lesoverzicht

Activiteit 1: **Hoe maak je een sterk paswoord**
Activiteit 2: **Hou het voor jezelf**
Activiteit 3: **Interland: Schattentoren**

Inleiding

Voor online privacy - en beveiligingsproblemen zijn er niet altijd duidelijke goede of slechte oplossingen. Je persoonlijke en privé-informatie beschermen - alle dingen die jou 'jou' maken, - betekent dat je de juiste vragen stelt en je eigen slimme antwoorden vindt.

Doelstellingen leerlingen

- ✓ **Ontdekken** waarom privacy belangrijk is en hoe het zich verhoudt tot onlineveiligheid.
- ✓ **Oefenen** hoe je sterke paswoorden maakt.
- ✓ **De hulpmiddelen** en instellingen bekijken die beschermen tegen hackers en andere bedreigingen.

Beveilig je geheimen
Woordenschat

Privacy: bescherming van je persoonlijke gegevens en die van anderen (ook wel gevoelige informatie genoemd)

Veiligheid: bescherming van de toestellen van mensen en de software die zich erop bevindt.

Tweestapsverificatie (ook wel tweefactorverificatie en tweestapsauthenticatie genoemd): een beveiligingsproces waarbij inloggen op een service twee stappen vereist. Je moet bijvoorbeeld je paswoord invoeren én een code invoeren die naar je mobiele telefoon is verzonden of een code van een app.

Paswoord of pascode: een geheime combinatie die wordt gebruikt om toegang te krijgen tot iets. Deze kan verschillende vormen aannemen; je kunt bijvoorbeeld een viercijferige numerieke code hebben voor je telefoon en een veel complexer paswoord voor je e-mailaccount. Een vuistregel is dat je je paswoorden zo lang en ingewikkeld mogelijk moet maken als je kunt, maar ze nog altijd moet kunnen onthouden.

Versleuteling: het proces waarbij informatie of gegevens worden omgezet in een code waardoor deze onleesbaar en ontoegankelijk wordt.

Complexiteit: de bedoeling wanneer je een veilig paswoord creëert. Een paswoord is bijvoorbeeld complex als het een mix is van cijfers, speciale tekens (zoals “$” of “&”) en zowel kleine als hoofdletters.

Hacker: een persoon die computers gebruikt om ongeoorloofde toegang te krijgen tot apparaten van andere mensen of organisatie en gegevens.

Beveilig je geheimen: Activiteit 1

Hoe maak je een sterk paswoord?

Kinderen leren hoe je een sterk paswoord maakt – en ervoor zorgt dat het geheim blijft.

Doelstellingen

- ✓ **Erkennen** dat het belangrijk is hun paswoorden enkel met de ouders/voogd te delen.
- ✓ **Meer weten** over paswoorden die apparaten en identiteit beschermen.
- ✓ **Begrijpen** hoe je paswoorden kan maken die moeilijk te raden zijn en die je gemakkelijk kunt onthouden.
- ✓ **De juiste beveiliging kiezen** voor aanmeldingsinstellingen en twee-factorverificatie overwegen.

Even praten

Voorkomen is beter dan genezen

Digitale technologie maakt het gemakkelijk om te communiceren met vrienden, klasgenoten, leraren en andere mensen. We kunnen op zo veel manieren contact leggen met de buitenwereld: via e-mail, sms en instant messages; in woorden, via foto's en filmpjes en met behulp van telefoons, tablets en laptops. (Hoe leg je contact met je vrienden?)

Maar dezelfde tools die het ons gemakkelijk maken om informatie te delen, maken het ook voor hackers en oplichters eenvoudig om die informatie te stelen en te gebruiken om onze apparaten, onze relaties en onze reputatie te beschadigen.

Beschermen betekent eenvoudige, slimme dingen doen, zoals schermvergrendeling op onze apparaten gebruiken, voorzichtig zijn met het plaatsen van persoonlijke informatie op apparaten die verloren of gestolen kunnen worden en vooral goede paswoorden kiezen.

- Weet iemand wat de twee meest gebruikte paswoorden zijn? (Antwoord: "1 2 3 4 5 6" en "paswoord".)
- Laten we brainstormen over enkele andere slechte paswoorden. (Voorbeelden: volledige naam, telefoonnummer, het woord 'chocolade'). Wie denkt dat dit sterke paswoorden zijn?)

Vervolg op de volgende pagina →

Activiteit

Laten we onze nieuwe vaardigheden oefenen door het paswoordspel te spelen.

1. Creëer paswoorden
Elk gezinslid krijgt 60 seconden om een paswoord te creëren.

2. Vergelijk paswoorden
Schrijf beide paswoorden op papier.

3. Stem!
Voor het beste en bespreek welk van beide het sterkst is.

Lessen

Dit is een idee om een extra veilig paswoord te creëren:

- Denk aan een leuke zin die je kan onthouden. Het kan je favoriete songtekst zijn, de titel van een boek, een quote uit een film, enz.
- Kies de eerste letters of de eerste twee letters van elk woord in de zin.
- Verander enkele letters in symbolen of getallen.
- Kies enkele letters in hoofdletters en enkele in kleine letters.

Het is belangrijk en leuk om sterke paswoorden te maken.

Richtlijnen om sterke paswoorden te creëren

Dit zijn enkele tips om paswoorden te creëren waarmee je je persoonlijke info/ geheimen beschermt.

Sterke paswoorden zijn gebaseerd op een beschrijvende zin die gemakkelijk te onthouden is en moeilijk door iemand anders te raden is – zoals de eerste letters van de woorden van een favoriete titel of lied, de eerste letters van een zin over iets wat je hebt gedaan – en bevatten een combinatie van letters, cijfers en symbolen Een voorbeeld: “Ik ging naar de lagere school in Brussel tot mijn 12 jaar” kan gebruikt worden om een paswoord te creëren: IgNdL$iBXLt12J.

Gewone paswoorden zijn paswoorden die sterk zijn en niet gemakkelijk te raden zijn door slechte software, maar kunnen worden geraden door iemand die jou kent (bijvoorbeeld, Ik ging naar de lagere school in Brussel).

Zwakke paswoorden gebruiken gewoonlijk persoonlijke informatie, zijn gemakkelijk te kraken en kunnen worden geraden door iemand die jou kent (bijvoorbeeld “IkhouvanLisa” of “Ikhouvanchocolade”).

DO’s

- Gebruik een uniek sterk paswoord voor elk van je belangrijkste accounts.
- Gebruik minimaal acht tekens, maar liefst veel meer (zolang je ze maar onthoudt!).
- Gebruik combinaties van letters (hoofdletters en kleine letters), cijfers en symbolen.
- Zorg ervoor dat je je paswoorden kunt onthouden, zodat je ze niet moet opschrijven, wat riskant is.
- Verander je paswoord meteen als je weet of denkt dat iemand anders dan een vertrouwde volwassene het kan weten.
- Gebruik altijd sterke schermbeveiligingen op je apparaten. Stel altijd automatisch vergrendelen in, voor het geval ze in verkeerde handen terechtkomen.
- Overweeg een paswoordbeheerder, bijvoorbeeld een die ingebouwd is in je browser, om je paswoorden te onthouden. Zo kun je een uniek paswoord gebruiken voor elk van je accounts en hoef je ze niet allemaal te onthouden.

DON’Ts

- Gebruik geen persoonlijke informatie (naam, adres, e-mail, telefoonnummer, RSZ-nummer, de meisjesnaam van je moeder, geboortedata, enz.), of gewone woorden in je paswoord.
- Gebruik geen paswoord dat makkelijk te raden is zoals je bijnaam, enkel de naam van je school, je favoriete voetbalteam, een cijferreeks (zoals 123456), enz. En gebruik zeker niet het woord “paswoord”!
- Deel je paswoord niet met iemand anders dan je ouders of je voogd.
- Schrijf paswoorden nooit ergens op waar iemand ze kan vinden.

Beveilig je geheimen: Activiteit 2

Hou het voor jezelf

Een ouder gebruikt een apparaat van de school om aan te tonen waar te kijken en waar te zoeken, wanneer je je privacyinstellingen aanpast.

Doelstellingen

- ✓ **Privacyinstellingen** aanpassen voor de onlinediensten die ze gebruiken.
- ✓ **Beslissingen** nemen over het delen van informatie op de sites en services die ze gebruiken.
- ✓ **Begrijpen** wat tweefactor- en tweestapsverificatie betekenen en wanneer je die moet gebruiken.

Even praten

Privacy staat gelijk aan veiligheid

Onlineprivacy en -beveiliging gaan hand in hand. De meeste apps en software bieden manieren om te bepalen welke informatie we delen en hoe.

Wanneer je een app of website gebruikt, zoek je naar een optie zoals 'Mijn account' of 'Instellingen'. Hier vind je de privacy- en beveiligingsinstellingen waarmee je kan beslissen:

• Welke informatie zichtbaar is op je profiel.
• Wie berichten, foto's, filmpjes of andere inhoud die je deelt, kan bekijken.

Door deze instellingen te leren gebruiken om je privacy te beschermen - en te onthouden ze up-to-date te houden - ben je zo veilig mogelijk online.
Het is belangrijk te weten dat je ouders of voogd deze beslissing altijd samen met jou nemen.

Activiteit

Wat je nodig hebt:

• Een toestel thuis waarmee u een voorbeeld kunt geven van wat geschikt geacht wordt voor kinderen (bijv. uw eigen e-mailaccount of die van uw kinderen).

1. Verificatieopties

Ik heb mijn laptop aangesloten op het projectiescherm. Laten we naar de instellingenpagina van deze app gaan. Hier zie je de keuzemogelijkheden:

• Je paswoord wijzigen
• Waarschuwingen ontvangen als iemand probeert in te loggen bij je account vanaf een onbekend apparaat
• Je onlineprofiel maken, inclusief foto's en filmpjes, alleen zichtbaar voor de door jou gekozen groepen familieleden en vrienden
• Tweefactorauthenticatie of tweestapsverificatie inschakelen

Vervolg op de volgende pagina →

2. Aanvullende verificatieopties

Laten we het hebben over tweestaps- en tweefactorverificatie.

- Tweefactorverificatie: wanneer je je aanmeldt op je account, zijn er twee stappen nodig. Zo moet je bijvoorbeeld je paswoord invoeren EN ontvang je een code per sms die je binnen 10 minuten moet invoeren voordat ze vervalt.
- Twee-factorverificatie: dit systeem vereist twee soorten informatie om je aan te melden. Het kan bijvoorbeeld vragen om je normale paswoord en vingerafdruk.

Welke privacy- en beveiligingsinstellingen zijn geschikt voor jou? Dat is iets om te bespreken met je ouder of voogd. Maar vergeet niet dat de belangrijkste beveiligingsinstelling in je hoofd zit: jij neemt de belangrijkste beslissingen over hoeveel, wanneer en met wie je persoonlijke gegevens wilt delen.

Lessen

Een sterk, uniek paswoord voor elk van je belangrijke accounts kiezen, is een goede eerste stap. Nu moet je ze onthouden en ook beveiligen.

Je paswoorden opschrijven, is niet per se een slecht idee. Maar doe je dit, laat dan geen papiertje met je paswoorden rondslingeren, bijvoorbeeld op je computer of bureau. Beveilig de lijst en bescherm jezelf door hem ergens te verbergen.

Beveilig je geheimen: Activiteit 3

Interland: Schattentoren

HELEEEEP! De toren is niet op slot, waardoor de waardevolle spullen van de Internaut, zoals persoonlijke informatie en paswoorden, een hoog risico lopen. Ontloop de hacker en bouw bij elke stap een onaantastbaar paswoord... om je geheimen voor eens en voor altijd te beveiligen.

Open je webbrowser op je desktop of mobiel apparaat (bijv. tablet) en ga naar https://beinternetawesome.withgoogle.com/nl_be/interland/tower-of-treasure.

Even praten

Laat uw kinderen de Schattentoren spelen en gebruik onderstaande vragen om te bespreken wat ze geleerd hebben in de game. De meeste kinderen hebben er het meest aan wanneer ze alleen spelen, maar u kunt ze ook in groepjes van twee laten spelen. Dit kan heel zinvol zijn voor jongere leerlingen.

- Wat zijn de elementen van een supersterk paswoord?
- Wanneer is het belangrijk om in het echte leven sterke paswoorden te creëren? Welke tips heb je geleerd over hoe je dit kan doen?
- Wat is een hacker? Beschrijf het gedrag van dit personage en hoe hij het spel beïnvloedt.
- Ga je je gegevens door de Schattentoren anders beschermen in de toekomst?
- Noem iets dat je anders gaat doen nadat je deze lessen hebt geleerd en het spel hebt gespeeld.
- Maak drie oefenpaswoorden die ‘supersterk’ zijn.
- Geef enkele voorbeelden van gevoelige informatie die je moet beschermen.