Achtergrondinformatie: Digitaal (veiligheid)

LET OP: De informatie in dit document kan dienen als naslagwerk tijdens het gebruik van de speelkaarten over digitale vaardigheden/veiligheid. De informatie in dit document correspondeert grotendeels met de informatie die wordt verschaft op de speelkaarten. Het is belangrijk op te merken dat de hier gepresenteerde informatie slechts een fractie vertegenwoordigt van de uitgebreide bronnen die beschikbaar zijn over dit onderwerp.

Het internet biedt een schat aan informatie en kansen, zeker op latere leeftijd. Dit thema onderzoekt de positieve aspecten van het internet, de middelen en kansen die het biedt. Het moedigt deelnemers aan om WhatsApp, video-oproepen, online bankieren en andere gangbare tools van de digitale wereld te verkennen. Het legt ook uit waarop je moet letten om online veilig te blijven, zoals het begrijpen van cookies, websitebeveiliging, phishing en malware. De spelkaarten combineren leuke zoekopdrachten met andere onderwerpen zoals voeding en sociale activiteiten om ervoor te zorgen dat digitale vaardigheden worden geïntegreerd met onderwerpen die relevant zijn voor de deelnemers. Bekijk het document – “voorbeelden van bijeenkomst activiteiten” om te zien hoe de je kaarten kan inzetten.

Enkele handige websites die gaan over ouderen en digitale vaardigheden

- https://www.seniorweb.nl
- https://ouderenfonds.nl/activiteit/digihulplijn/
- https://www.veiligdigitaal.com/hulp-nodig

Wat is betrouwbare informatie?

Tijdens deze gehele cursus combineren wij inhoudelijke onderwerpen met online zoekopdrachten en informatie. Bijvoorbeeld over gezonde voeding, lichamelijke veroudering of activiteiten in de buurt. Het is echter soms best lastig om te onderscheiden welke websites betrouwbare informatie vertellen en welke niet. Zeker met de opkomst van sociale media gaan er soms de wildste verhalen de ronde over diëten en voedingssupplementen. Daarnaast zijn niet alle gezondheidswebsites onafhankelijk. Wist je bijvoorbeeld dat Etos enkele gezondheidswebsites (zoals gezondheidsplein.nl en ziekenhuis.nl) heeft overgenomen? Ook al werken zij nauw samen met huisartsen om hun informatie goed te keuren, hun websites zijn dus niet volledig onafhankelijk zonder enig winstoogmerk zoals Thuisarts dat wel is.

Het is belangrijk om samen met de deelnemers te kijken hoe ze kunnen onderzoeken welke sites en informatie betrouwbaar is en welke niet. Een handige checklist over voedingsadvies is te vinden op de website van het voedingscentrum via deze link.

Hieronder zijn enkele betrouwbare links waar deelnemers naar verwezen kunnen worden als het gaat om gezondheid en voeding:

- Thuisarts
- Voedingscentrum
- RIVM
- Nederlandse Vereniging van Diëtisten

Daarnaast heeft Pharos veel informatie en hulpbronnen als het gaat om gezondheid en gezondheidsverschillen voor professionals. Zo ook veel informatie in diverse talen en voor diverse doelgroepen.

TIP: indien Google gebruikt wordt om websites te zoeken dan is het verstandig om de websites waar *ad* voor staat over te slaan. Ondanks dat dit soms nuttige websites zijn kunnen het ook commerciële websites zijn die Google betalen om bovenaan te staan. Ga dus voor de zekerheid altijd voor de eerste optie zonder *ad.*

Als het gaat om digitale veiligheid zijn er een paar concepten om op te letten:

1. *Malware* - Dit verwijst naar schadelijke software die onze digitale apparaten kan infecteren. Malware wordt vaak verspreid via berichten (e-mail, sociale media, WhatsApp of sms) met bestanden, bijlagen of links. Zodra deze elementen zijn gedownload en uitgevoerd, kunnen ze je digitale apparatuur compromitteren.

2. *Phishing* - Phishing omvat frauduleuze pogingen om organisaties zoals banken of overheidsinstellingen na te bootsen, met als doel toegang te krijgen tot gevoelige informatie zoals wachtwoorden of financiële gegevens. Phishing-berichten bevatten vaak dringende waarschuwingen, bijvoorbeeld over een aanstaande beindiging van een service als u niet nu inlogt via de link die ze sturen.

Video suggestie phishing:
https://www.youtube.com/watch?v=0pU2866IT1Y&list=PLRrydbbne6HPpz6FpazC9MUyR_ixcrFqA&index=6

TIP: dit filmpje kunt u ook tonen tijdens de bijeenkomst. Vaak maakt het kijken van een verhaal van een andere oudere veel los en verlaagt het de drempel voor deelnemers om hun eigen ervaringen te delen over dit onderwerp.

3. *Oplichting* - Oplichting heeft het doel zoveel mogelijk persoonlijke informatie te verkrijgen en draait vaak om vervalste loterijwinsten, valse erfenisclaims of

jobaanbiedingen waarbij voorafbetalingen vereist zijn. Op deze manier verkrijgen de oplichters persoonlijke informatie zoals betaalgegevens.

4. *Afpersing* - Bij afpersingspogingen proberen dreigende partijen slachtoffers af te persen door te beweren dat ze compromitterende inhoud of persoonlijke informatie bezitten en dreigen deze openbaar te maken tenzij er losgeld wordt betaald. Vaak is het zo dat de compromitterende inhoud die in deze dreigingen wordt gebruikt helemaal niet bestaat.

5. *Spoofing* - Spoofing is een truc waarbij een oplichter zich voordoet als een medewerker van je bank, een helpdesk, webwinkel of van een overheidsinstantie. Als je geld overmaakt, komt dat terecht bij de oplichter.

Video suggestie Spoofing: https://www.youtube.com/watch?v=aDniKxJzEYY

Voor tips om criminelen te slim af te zijn, of voor andere vragen over oplichtingspraktijken, kunnen ouderen bellen naar de Advieslijn Veiligheid: 0348-238591. Deze lijn is onderdeel van de ANBO.

Wees extra alert als:

- Je berichten ontvangt van onbekende of onverwachte bronnen.
- Het e-maildomein niet overeenkomt met het bedrijf/instelling/dienst dat het bericht verzendt;

Voorbeeld: als je een bericht ontvangt van een officiële organisatie, zou je verwachten dat het e-mailadres van de afzender eruitziet als: contact@bank.com en niet als: john.johnson@boatsandsea.com. Wees dus alert als het e-mailadres van de afzender niet overeenkomt met de organisatie.

- Je inhoud tegenkomt die je onder druk zet om onmiddellijke actie te ondernemen.

Voorbeeld: "als je dit niet doet, wordt de service binnen x uur geannuleerd."

- Je onpersoonlijke communicatie in de berichtinhoud tegenkomt. Legitieme organisaties gebruiken meestal een persoonlijke vorm van communicatie, bijvoorbeeld het gebruik van achternamen.
- Het bericht bijlagen of een link bevat.
- Het bericht spelfouten bevat.
- Er uitdrukkingen worden gebruikt die ongebruikelijk zijn.

Doe het zelf!

Tijdens de bijeenkomst kunt u gebruik maken van de deze quiz. Hiermee kunt u samen met de deelnemers oefenen hoe ze neppe van echte berichten kunnen onderscheiden.

Op de website Veilig Internetten vindt u meer quizzen over het thema digitale veiligheid.

Beveiligingstips *Algemeen*

- Voer regelmatig een software-update uit (digitale apparaten geven je daar een melding van).
- Controleer de privacy-instellingen van je digitale apparaten, je sociale media-account en e-mail.
- Gebruik dubbele authenticatie om toegang te krijgen tot sociale media, e-mail, internetbankieren, enz.
- Verwijder accounts die niet meer in gebruik zijn, bijvoorbeeld als je je Facebook-profiel niet gebruikt, kun je het account verwijderen.
- Een veilige en betrouwbare institutionele website heeft contactgegevens, zoals een adres, een telefoonnummer, een e-mailadres of een contactformulier.

Online winkelen

- Gebruik bepaalde services alleen als je zeker weet dat je bent verbonden met een veilig wifi-netwerk. Bijvoorbeeld, wanneer je toegang hebt tot je internetbankrekening, zou je dit alleen thuis moeten doen en niet vanaf een openbare plaats waar je niet zeker bent van de veiligheid van het netwerk.
- Doe online winkelen alleen op bekende en geverifieerde websites.
- Als de website om persoonlijke informatie vraagt, moet je controleren of het adres begint met "https" - dit staat voor Hypertext Transfer Protocol Secure - of dat er een slotpictogram naast het adres staat.
- Controleer regelmatig je bankrekening om ongebruikelijke activiteiten op te sporen, zoals geldopnames waarvan je niet op de hoogte bent of die je niet hebt toegestaan.

De C&A (ja van de kleding) heeft een handige website over veilig online shoppen: https://www.c-and-a.com/nl/nl/shop/veilig-online-shoppen
Of deze link van de politie: https://www.vraaghetdepolitie.nl/misdaad-en-geweld/hoe-weet-jeof-je-bij-een-betrouwbare-webshop-koopt.html

Wachtwoorden

- Deel je wachtwoorden niet met anderen.
- Gebruik geen persoonlijke informatie om een wachtwoord te maken, zoals geboortedatum of adres.
- Verander je wachtwoorden regelmatig.

- Gebruik voor verschillende accounts verschillende wachtwoorden, bijvoorbeeld één voor sociale media, een andere voor e-mail, enz.
- Probeer een complex wachtwoord te creëren, bijvoorbeeld een zin met cijfers en symbolen zoals "itsapieceofcake#2022".
- Houd een notitieboekje met alle wachtwoorden geschreven en verborgen op een veilige plaats.

E-mail / sociale media / WhatsApp / sms

- Wees voorzichtig met links die via e-mail en/of berichten worden verzonden.
- Officiële organisaties sturen meestal geen links, maar vragen de gebruiker om toegang te krijgen tot de service via hun officiële website.
- Wees voorzichtig met e-mails die niet worden verwacht of die de referentie in de inhoud hebben met iets "dringends".
- Download geen bijlagen en klik niet op links die in e-mail- of sms-berichten verschijnen.
- Als je vermoedt dat een bericht afkomstig is van een vervalste afzender, kun je de authenticiteit van de informatie verifiëren via een andere bron, zoals een telefoongesprek met de verzendende organisatie.

Het delen van (persoonlijke) informatie

- Alles wat online wordt gepost en gedeeld, blijft daar voor altijd.
- Vermijd het delen/posten van persoonlijke informatie.
- Vermijd het delen/posten van foto's.
- Vermijd het delen/posten van statusupdates.
- Voorbeeld: een bericht plaatsen over je huidige vakantie kan aangeven dat je huis onbeheerd is achtergelaten.
- Wanneer je iets online plaatst of deelt, kan die informatie worden gebruikt om je gewoonten en routines te volgen, wat je kwetsbaarder maakt voor oplichting en fraude.
- Praat niet met vreemden online.
- Voeg onbekende mensen niet toe aan je sociale media.