Digi Dinsdag – Veilig (zoeken) op het internet

Tips & Checks

1. Zorg voor veilige wachtwoorden

Tip 1. Gebruik geen namen van huisdieren, beroemdheden, etc.

Tip 2. Gebruik geen persoonlijke informatie, zoals verjaardag, naam, e-mail, etc.

Tip 3. Gebruik geen patronen & opeenvolgingen, zoals qwerty, asdf, 123456, abc123, …

Tip 4. Gebruik geen namen van voetbalclubs of woordenboekwoorden, zoals “voetbal”, “wachtwoord”, “hallo”, “meester”, …

Tip 5. Gebruik geen namen van (klein)kinderen, deze zijn via sociale media makkelijk terug te vinden.

Tip 6. Maak een wachtwoordenboekje
- *Bewaar het boekje op een veilige plek, bijvoorbeeld in de kluis.*
- *Schrijf uw wachtwoorden **cryptisch** op, zodat anderen het niet herkennen:*
- *Inlognaam en wachtwoord op andere plek.*

TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

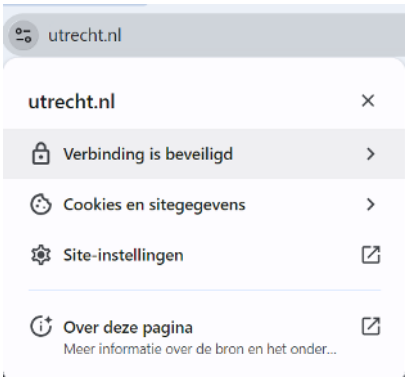
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

2. Gebruik waar mogelijk tweestaps-verificatie

- Dit kan via sms (er wordt een code per sms naar je telefoon gestuurd)
- Of via een Authenticator app

3. Kijk of een website veilig is

- Bij een veilige website begint de link met: https (s staat voor secure)
- Ook staat er een slotje of dit symbool aan het begin van de link
- Voorbeeld https://www.utrecht.nl/



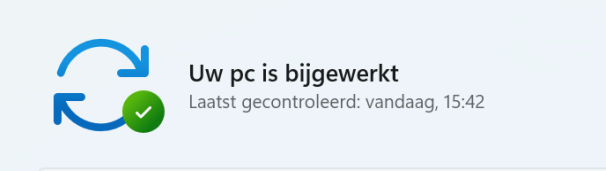
4. Wat wel en niet doen met openbare wifi netwerken

- Niet inloggen bij sites zonder slotje (geen versleuteling van gegevens)
- Geen persoonlijke gegevens invoeren
- Geen financiële handelingen verrichten, zoals internetbankieren.
- Een vertrouwde locatie betekent niet meteen een vertrouwd Wifi-netwerk.
- Schakel automatisch verbinden uit en ‘vergeet’ openbare wifi nadat je het hebt gebruikt.

5. Doe je updates

- Hoeveel apparaten gebruikt u die aangesloten zijn op internet? Zorg dat deze altijd up-to-date zijn en stel deze updates niet uit.

- Updaten is ALTIJD NOODZAKELIJK: Denk aan laptops, desktops, smartphones, tablets. Maar ook huishoudelijke apparaten die zijn aangesloten op het internet (zoals thermosstaten, lampen en stereo)



6. Gebruik een virus-scanner

- Gebruik een virusscanner om je computer regelmatig te scannen. U kunt instellen dat dat automatisch gaat.
- De virusscanner van Microsoft (is Defender) is op zich heel goed maar een externe virusscanner kan nog altijd nuttig zijn om te gebruiken.
- De meeste virusscanners kunnen inmiddels ook onveilige websites herkennen.
- Betaald of gratis? Voorbeelden van goede gratis virusscanners zijn Bitdefender en Kaspersky.

7. Maak regelmatig een back-up

Waarom een back-up maken?

- Bij besmetting met een virus zijn uw bestanden veilig
- Als uw apparaat kapot gaat bent u niet alles kwijt
- Als uw systeem wordt overgenomen met ransom ware

Hoe maak ik een back-up?

- Externe harde schijf
- In “de Cloud”

Voordelen van werken in de Cloud:

- Je kunt altijd en overal bij je bestanden
- Je bestanden staan veilig op het internet
- Je hebt geen aparte apparaten nodig voor back-ups

Nadelen van werken in de Cloud:

- Je hebt altijd een internetverbinding nodig
- Je bent ‘overgeleverd’ aan grote bedrijven zoals Google en Microsoft

8. En altijd “Eerst checken, dan klikken”

Als je een e-mail ontvangt…

Weet je wanneer je moet opletten?

- Er wordt je gevraagd om geld over te maken.
- Er wordt je gevraagd om in te loggen of om je persoonsgegevens te mailen.
- Er is haast bij.

Als dit het geval is weet je voortaan wat je te doen staat! Eerst checken, dan klikken! Klik niet zomaar op een link.

Weet je wat je moet checken?

- Check de URL (het adres) van een link door er met er met je muis op te gaan staan (niet klikken natuurlijk!). Kijk goed of je vreemde dingen (rare tekens, vreemde woorden) in de URL ziet staan.
- Check het e-mailadres van de afzender.
- Krijg je een onverwacht betaalverzoek van een bekende? Bel op en vraag of het klopt.
- Krijg je een betaalverzoek van een bedrijf? Bel het bedrijf op om te vragen of het klopt.

Twijfel je of een website veilig is? Je kunt de link checken via:

- https://www.checkjelinkje.nl/
- https://api.whatsapp.com/message/6FDVTLUV5W4ND1

Waar moet je op letten bij online shoppen / webshops ?

- De bekende webshops hebben een keurmerk:
- Check altijd of het een beveiligde website is.
- Bijvoorbeeld: https://www.bol.com/nl/nl/

Gebruik vergelijking sites met aanvullende informatie over de webshop:

- Service - Levertijd - Reviews
- https://www.kieskeurig.nl/ of https://tweakers.net/
- Een regel die je kunt hanteren: Als iets te mooi is om waar te zijn, is het dat meestal ook!
- Gaat u vaker naar een website? Sla deze dan op onder “favorieten”

Meer informatie over veilig internetten en hulp/advies:

- www.digihulp.nl
- www.veiliginternetten.nl
- www.seniorenweb.nl
- https://www.digitale-weerbaarheid.nl/

Co-funded by the European Union