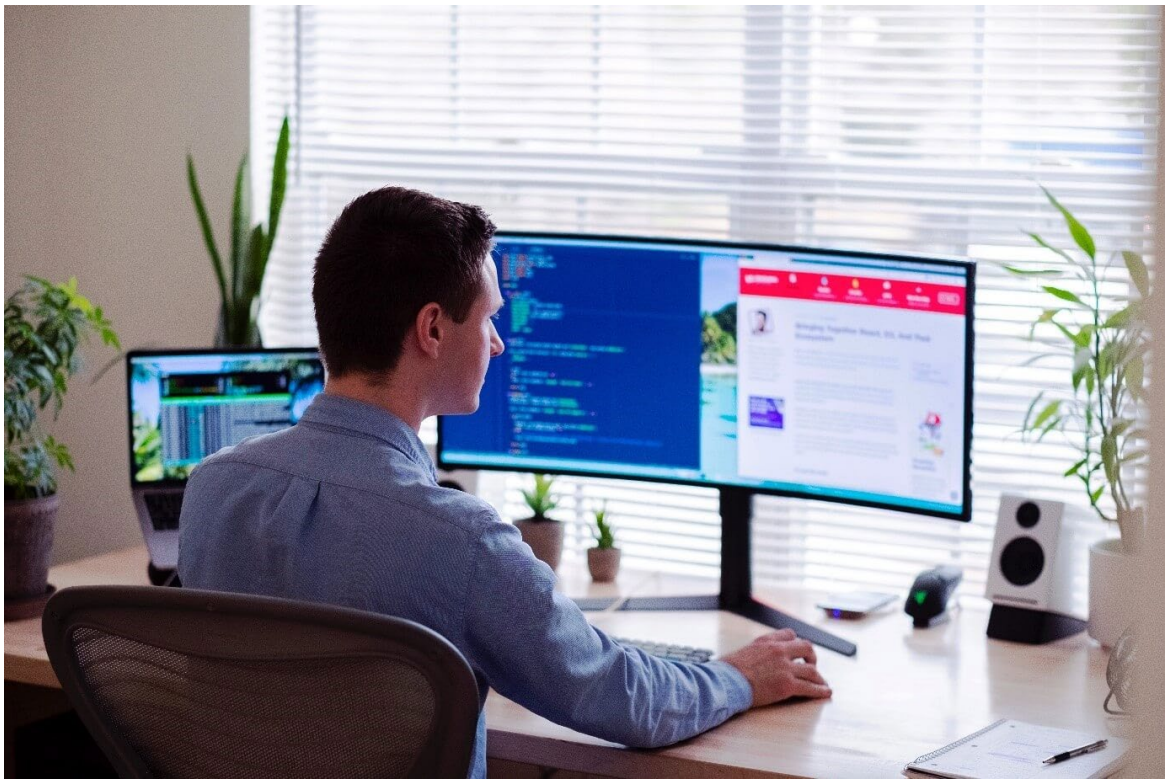

ONLINE BEDREIGINGEN VOORKOMEN

AAN DE SLAG MET DIGITALE VAARDIGHEDEN
TRAINING: INFORMATIEBEVEILIGING EN PRIVACY

DIGIVAARDIG IN DE ZORG

ONLINE BEDREIGINGEN VOORKOMEN

In dit werkblad leer je welke online bedreigingen je kunt tegenkomen als je met computers op het internet werkt. Gelukkig zijn er ook genoeg manieren om je te wapenen tegen deze dreigingen. Weet jij wat de verschillende termen betekenen?

Opdracht 1

Wie werkt met de computer op het internet wordt vaak gewaarschuwd voor de risico's en online bedreigingen. Welke risico's ken jij?

Opdracht 2

Wat doe jij of de organisatie waar je werkt om deze online bedreigingen te voorkomen? Kruis aan wat van toepassing is.

- ☐ Regelmatig wijzigen van wachtwoorden
- ☐ Updates van software automatisch uitvoeren
- ☐ Inloggen op systeem middels twee-stap verificatie
- ☐ Anders namelijk:

Opdracht 3

Wat kun je het beste doen als je het vermoeden hebt dat er iets mis is met jouw computer en dit risico geeft op informatiebeveiliging?

A. ◯ Direct de ICT Servicedesk van de organisatie bellen
B. ◯ Melding maken bij de Autoriteit Persoonsgegevens (AP)
C. ◯ Zelf op onderzoek uit via een zoekmachine op het internet
D. ◯ Laptop afsluiten en opnieuw opstarten

Opdracht 4

Bekijk onderstaande beschrijvingen en zoek de bijpassende computerterm bij elkaar. Verbind de termen door de cijfers (1 t/m 6) te koppelen aan de letters (a t/m f). De antwoorden vind je aan het einde van dit werkblad.

1. Mensen verleiden om op een valse website nietsvermoedend persoonlijke gegevens in te voeren.

2. Een veilige(re) manier van inloggen doordat er op twee manieren wordt geverifieerd of jij het bent die wilt inloggen.

3. Bewaakt het inkomend en uitgaand netwerkverkeer. Bepaalt welk verkeer betrouwbaar is en welk verkeer gevaarlijk is.

4. Het gijzelen van bestanden door deze te versleutelen met als doel deze later te ontsleutelen in ruil voor losgeld.

5. Het inbreken in computersystemen, persoonlijke accounts, computernetwerken of digitale apparaten.

6. Zorgt voor een beveiligde verbinding tussen jouw apparaat en een plek ergens op het internet. Hierdoor kan niemand meekijken.

A. Hacken

B. VPN-verbinding

C. Phishing

D. Ransomware

E. Twee-stap authenticatie

F. Firewall

Antwoorden opdracht 3

A. Bij een vermoeden op het lekken van vertrouwelijke informatie van de organisatie bel je de ICT servicedesk. Zij zulle als het nodig is overleggen met de functionaris gegevensbescherming. Een werknemer doet zelf geen melding bij de AP.

Antwoorden opdracht 4

1. C
2. E
3. F
4. D
5. A
6. B

Deze module is gemaakt door Xiomara Vado Soto voor Digivaardig in de Zorg in samenwerking met Daan Brinkhuis van 's Heeren Loo.

Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl.