ORDLISTE – DIGITAL SIKKERHED

1. **Firewall**
   Forklaring: En sikkerhedsbarriere, der overvåger og kontrollerer indgående og udgående netværkstrafik.

2. **Malware**
   Forklaring: Skadelig software designet til at forstyrre, beskadige eller få uautoriseret adgang til et system.

3. **Phishing**
   Forklaring: En svindelmetode, hvor angribere udgiver sig for at være troværdige enheder for at stjæle følsomme oplysninger.

4. **Kryptering**
   Forklaring: Processen med at kode information, så kun autoriserede parter kan læse den.

5. **VPN** (Virtual Private Network)
   Forklaring: En tjeneste, der krypterer din internettrafik og skjuler din online identitet.

6. **To-faktor autentificering** (2FA)
   Forklaring: En sikkerhedsproces, der kræver to forskellige former for identifikation for at få adgang.

7. **Hacker**
   Forklaring: En person, der får uautoriseret adgang til computersystemer, enten med ondsindede eller etiske formål.

8. **DDoS-angreb** (Distributed Denial of Service)
   Forklaring: Et angreb, der overbelaster et system eller netværk for at gøre det utilgængeligt for brugere.

9. **Antivirus**
   Forklaring: Software designet til at detektere, forhindre og fjerne malware.

10. **Patch**
    Forklaring: En softwareopdatering designet til at løse sikkerhedsproblemer eller forbedre et program.

11. **Sårbarhed**
    Forklaring: En svaghed i et system, der kan udnyttes af en angriber.

12. **Penetrationstestning**
    Forklaring: En autoriseret simuleret cyberangreb for at evaluere sikkerheden i et system.

13. **Ransomware**
    Forklaring: Malware, der krypterer offerets filer og kræver løsepenge for at dekryptere dem.

14. **Social engineering**
    Forklaring: Manipulationsteknikker, der udnytter menneskelig psykologi for at få adgang til systemer eller data.

15. **Zero-day sårbarhed**
    Forklaring: En softwaresårbarhed, der er ukendt for softwareudvikleren og potentielt kan udnyttes af hackere.

16. **Databrud**
    Forklaring: En sikkerhedshændelse, hvor følsomme, beskyttede eller fortrolige data bliver set, stjålet eller brugt af en uautoriseret person.

17. **Endpoint-sikkerhed**
    Forklaring: Beskyttelse af netværksenheder som computere, mobiltelefoner og tablets mod cybertrusler.

18. **Adgangskontrol**
    Forklaring: Metoder og politikker til at begrænse adgang til systemer og data baseret på brugeridentifikation og autorisation.

19. **Biometrisk autentificering**
    Forklaring: Brug af unikke biologiske karakteristika (f.eks. fingeraftryk eller ansigtsgenkendelse) til at verificere en persons identitet.

20. **GDPR** (General Data Protection Regulation)
    Forklaring: EU's databeskyttelsesforordning, der regulerer behandling og beskyttelse af personoplysninger.