WAT IS CYBERCRIME?

Cybercrime is een vorm van digitale criminaliteit waarbij internetcriminelen inbreken op bijvoorbeeld een computer, telefoon of het complete netwerk van een organisatie. ICT is bij deze vorm van criminaliteit het doel én het middel. De motieven van internetcriminelen lopen uiteen. Veelal is dit om een grote hoeveelheid geld buit te maken of om een bedrijf schade aan te brengen. De impact is over het algemeen enorm.

Vormen cybercriminaliteit

Er zijn verschillende soorten cybercrime waarmee u te maken kunt krijgen. Hieronder staan de 10 meest voorkomende varianten.

1. **Cyberafpersing**
   Zodra hackers toegang hebben tot het digitale netwerk starten zij met het afpersen van de organisatie of een persoon. U krijgt pas weer toegang tot de computer(s) of telefoon(s) zodra er geld betaald is.
2. **Cyberstalking**
   Deze vorm van cybercrime komt vaak voor bij individuen: via digitale kanalen word je stelselmatig lastiggevallen.
3. **Phishing**
   Dit is een vorm van cybercrime die we steeds vaker zien: via een valse e-mail of website wordt gevraagd naar uw persoonlijke gegevens. Internetcriminelen kunnen dit ook vanuit uw bedrijfsnaam doen. Geef nooit zomaar wachtwoorden, pincodes of andere persoonlijke gegevens door naar aanleiding van dit soort berichten.
4. **Malware**
   Malware is een verzamelnaam voor schadelijke software. Door de computer te besmetten met malware kunnen criminelen toegang krijgen tot de computer en uw bestanden vergrendelen. Een bekend voorbeeld van malware is het virus. Een virus is een computerprogramma dat zich in een bestand op uw computer nestelt. Er kan informatie op uw computer verspreid worden, maar het is ook mogelijk dat uw computer hierdoor niet meer te gebruiken is.
5. **Password cracking**
   Criminelen achterhalen uw wachtwoorden om vervolgens in te breken op uw computer, telefoon en/of netwerk.
6. **Botnet**
   Een botnet is een netwerk van geïnfecteerde computers die aangestuurd worden door een centrale server. Een internetcrimineel koopt toegang tot dit netwerk en kan automatisch opdrachten uitvoeren.
7. **Defacing**
   Bij defacing veranderen cybercriminelen de content: bijvoorbeeld door de homepage van uw website aan te passen.
8. **Identiteitsfraude**
   Deze vorm van cybercrime kan bij zowel individuen als bedrijven voorkomen. Internetcriminelen gebruiken uw identiteit of bedrijfsgegevens om bijvoorbeeld producten of diensten te bestellen, creditcards aan te vragen of illegale activiteiten uit te voeren.
9. **Ransomware**
   Een vorm van cybercrime waarbij bestanden op je computer vergrendeld worden. Wilt u weer toegang tot de gegevens? Dan moet er, de naam zegt het al, losgeld betaald worden.
10. **DdoS-aanval**
    Bij een DdoS-aanval wordt de server overbelast met als doel de website of internetdienst onbruikbaar te maken.

Doel van internetcriminelen

Cybercriminelen of hackers zijn er in vele soorten en maten: van personen tot organisaties en van activisten (zoals de hackersgroep Anonymous) tot staatsgebonden groepen. In werkelijkheid gaat het vaak om personen of collectieven die het internet gebruiken om te protesteren en mensen te mobiliseren of om individuen of bedrijven te chanteren of deels af te persen met het doel geld te verdienen.