



## **Veilig gebruik van je laptop met mobiel internet**

### **Waarom je laptop beveiligen?**

Je laptop staat vol met persoonlijke informatie. Bijvoorbeeld je adressenlijst, mail, agenda en documenten. Als je niet oplet bestaat de kans dat anderen deze informatie ongewild in hun bezit krijgen. Dit kun je voorkomen door onderstaande tips op te volgen. En natuurlijk is het slim om een verzekering af te sluiten voor je laptop, zodat je geen zorgen hoeft te maken over schade of verlies.

Tips voor veilig gebruik van je laptop met mobiel internet

### **Houd je laptop up-to-date**

Installeer de laatste software updates. Zorg ervoor dat je altijd de laatste update van het besturingssysteem (Windows, Mac etc.) op jouw computer hebt geïnstalleerd. Met de update wordt namelijk ook de beveiliging bijgewerkt. De meeste besturingssystemen kunnen dit automatisch. Vanwege kosten en bandbreedte kun je dit het best via je vaste internet verbinding doen. Software updates zijn meestal onderdeel van de licentie-overeenkomst van uw software en brengen normaal gesproken geen extra kosten met zich mee."

### **Gebruik antivirus software**

Installeer antivirus software op je laptop en houd deze up-to-date. Hiermee voorkom je dat jouw laptop via de e-mail met een virus kan worden besmet. Afhankelijk van jouw eigen wensen download je een gratis virusscanner of koop je een pakket met volledige bescherming dat je enkele tientallen euro's per jaar per systeem kost.

### **Activeer de firewall**

Activeer de firewall op het besturingssysteem van je laptop of installeer additionele firewall software. Een Firewall filtert ongewenst internetverkeer voordat het jouw systeem bereikt en schade kan aanrichten.

### **Open geen onbekende bestanden die je niet vertrouwt**

Open geen bestanden in de e-mail die je niet vertrouwt en installeer geen onbekende toepassingen. Onbekende bestanden kunnen een virus bevatten.

### **Wees zuinig op je e-mailadres**

Verstrek jouw e-mailadres alleen aan partijen die je vertrouwt. Als je jouw e-mailadres bij meer partijen achterlaat wordt de kans dat je (ongewenst) spam e-mail gaat ontvangen groter.

### **Mail geen vertrouwelijke informatie**

Geef geen vertrouwelijke informatie zoals pincodes, gebruikersnaam, wachtwoorden, bankrekeningnummers of creditcardnummers aan derden via de e-mail. Vertrouwde instanties zoals banken, creditcard maatschappijen of KPN vragen nooit per e-mail om jouw wachtwoord. Laat deze gegevens ook niet achter op websites die je niet vertrouwt.

### **Gebruik een pincode op de simkaart**

Gebruik een pincode op de simkaart in jouw Mobiel Internet Kaart of Dongel. Wanneer je de simkaart of het Mobiel Internet Kaart verliest, voorkom je dat anderen ongewenst gebruik van je abonnement op jouw kosten gaan maken. Laat direct simkaart blokkeren door KPN als je simkaart is gestolen. De klantenservice bij diefstal is 24 uur per dag bereikbaar op: 06 1200 1200.



### **Bewaar je IMEI nummer goed**

IMEI is de afkorting van International Mobile Equipment Identification. Het is het serienummer van je Mobiel Internet Kaart of Dongel. Het IMEI-nummer op de sticker van je Mobiel Internet Kaart of Dongel. Met je IMEI kan de politie een gestolen apparaat een sms bombardement sturen.

### **Gebruik een wachtwoord op je laptop**

Zet een wachtwoord op jouw laptop. Hiermee voorkom je dat anderen ongewenst informatie op jouw laptop kunnen lezen, of dat bij diefstal vertrouwelijke informatie in handen van derden komt. Kies geen al te voor de hand liggende wachtwoorden en wijzig ze regelmatig.

### **Aanvullende beveiliging**

Gebruik aanvullende beveiliging wanneer je via mobiel internet inlogt op jouw bedrijfsnetwerk, bijvoorbeeld via een VPN. Hiermee voorkom je dat jouw gegevens gelezen kunnen worden door derden. Voor iedere bedrijfssituatie zijn verschillende oplossingen beschikbaar. Kijk op [kpn.com/zakelijk](https://kpn.com/zakelijk) voor meer informatie daarover.

## **Termen en uitleg**

Er zijn verschillende vormen van digitale misbruik, hieronder lichten we de meest voorkomende toe.

### **Hackers**

Hackers zijn personen die inbreken op jouw computer om persoonlijke informatie te achterhalen of je pc te misbruiken voor illegale activiteiten.

### **Spam**

Spam is ongewenste e-mail die erop gericht is om je een product of dienst te verkopen, zonder dat je hierom gevraagd hebt.

### **Phishing**

Phishing is een verzamelnaam voor e-mail of internetpagina's die zich voordoen als vertrouwde instellingen en bedrijven maar dat in werkelijkheid niet zijn. Vaak lijken ze op bank- of veilingssites. Ze stellen je vragen over wachtwoorden of een creditcardnummer om te misbruiken en geld of gegevens van je te stelen. KPN vraagt nooit om je wachtwoorden. Wordt er wel om je wachtwoord of pincode gevraagd, ga hier dan niet op in en meld dit bij de afdeling Abuse van KPN.

### **Spyware**

Spyware is software die zich ongezien op jouw computer nestelt om internetgedrag in de gaten te houden. Deze informatie wordt gebruikt om gerichte spam of pop-ups te versturen of jouw persoonlijke gegevens -bijvoorbeeld banknummers- te achterhalen en te verkopen of te misbruiken.

### **Virussen**

Virussen zijn kleine programma's die zich verstoppen in bestanden. Bijvoorbeeld foto's of bestanden die je per e-mail ontvangt. Op je computer kunnen ze schade aanrichten door bestanden te beschadigen of verwijderen.

### **Wormen**

Een worm is een virus met een extra eigenschap. Wormen richten niet alleen schade aan op jouw computer, maar gebruiken jouw computer ook nog eens om zich te verspreiden. Ook hebben zij geen bestanden nodig om zich aan te hechten. Terwijl je op internet surft, kan jouw pc ongemerkt geïnfecteerd worden.

### **Trojaans paard**

Een Trojaans paard is een slim computerprogramma dat je pc overneemt. Zo kan het jouw



computer gebruiken om spam te versturen, zelfs zonder dat je het door hebt. Meestal wordt jouw computer onderdeel van een botnet. Dat is een groep van pc's die gezamenlijk misbruikt worden. Een Trojaans paard kan, net als een worm, je computer infecteren zonder dat je het door hebt.