Checklist

Veilig omgaan met persoonlijke data

10 tips voor op de werkplek

Wolters Kluwer

In je werk kom je regelmatig in aanraking met (gevoelige) gegevens van je klanten of medewerkers. Natuurlijk ga je daar zorgvuldig mee om. Toch kunnen kleine vergissingen ervoor zorgen dat je data op straat komt te liggen: een datalek.

In 2018 is de Algemene Verordening Gegevensbescherming (AVG) ingevoerd om persoonsgegevens te beschermen. Sindsdien heeft de Autoriteit Persoonsgegevens al duizenden klachten ontvangen en ook al wat boetes uitgedeeld. Het is dus heel belangrijk dat je voorzichtig blijft omgaan met persoonlijke data.

Deze tien tips helpen je om veilig met data om te gaan:

1 **Check je e-mails.**

Verreweg de meeste datalekken gebeuren door foutjes met e-mailen: een bestand naar een verkeerde ontvanger of een tikfout in een e-mailadres. Wees alert als je privacygevoelige data verstuurt. Kijk ook kritisch naar de inhoud van je e-mails, vooral als je berichten doorstuurt. Welke gegevens staan daar in, en zijn die relevant voor de volgende ontvanger?

2 **Wees voorzichtig met e-mailbijlagen.**

Een document vol persoonsgegevens als bijlage naar iemand anders e-mailen is niet volledig veilig. Vergrendel bijlagen met grote hoeveelheden persoonlijke informatie met een wachtwoord. Deel dat wachtwoord niet in de e-mail, maar bijvoorbeeld separaat per sms of telefoon. Vind je dit in bepaalde gevallen ondoenlijk? Maak hierover dan goede afspraken met je werkgever of je klanten.

3 **Gebruik software om wachtwoorden op te slaan.**

Wachtwoorden onthouden is lastig. Veel mensen gebruiken daarom steeds dezelfde wachtwoorden, laten de laptop of smartphone wachtwoorden onthouden of ze slaan ze op in een mail of document. Dat is niet veilig. Gebruik software die helpt bij het onthouden van moeilijke maar veilige wachtwoorden, zoals Lastpass of 1Password. Je werkgever kan je hierbij helpen.

4 **Maak duidelijke afspraken over welke software je gebruikt.**

In je dagelijks werk gebruik je diverse soorten software. Bijvoorbeeld programma's om bestanden te delen, zoals WeTransfer en Dropbox. Wees je ervan bewust dat niet alle software veilig omgaat met gegevens. Betaalde software van Microsoft, zoals Office 365, is in veel gevallen veiliger dan gratis software (waarbij je vaak betaalt met je data).

5 **Print veilig en vergrendel je apparaat.**

Print persoonlijke documenten alleen via een printer met een pincode of een persoonlijke pas. Zo kan alleen degene die de documenten heeft afgedrukt, ze ophalen bij de printer. Vergrendel bovendien altijd je computer of laptop als je er niet achter zit.

6 **Gebruik goede wachtwoorden.**

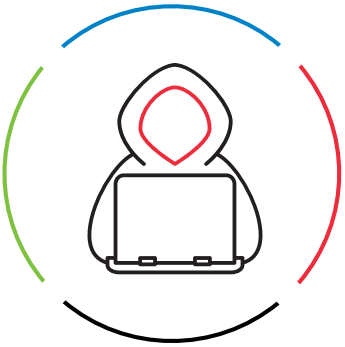
Zorg dat je een goed wachtwoord gebruikt voor je computer of laptop. Wachtwoorden als 'welkom1234' of de naam van je kind zijn niet veilig. Goede wachtwoorden zijn lang en bestaan uit letters, hoofdletters, cijfers en/of speciale tekens. Extra tip: vervang in je wachtwoord bepaalde letters door tekens die erop lijken. Bijvoorbeeld Ditis€€nG0€d_W@cht-w00rd!

7 **Werk buiten de deur via een veilige verbinding.**

Even in de trein de vergadering voorbereiden? Als je je computer aan een openbaar wifinetwerk verbindt zonder een VPN-verbinding te gebruiken, kunnen anderen heel gemakkelijk toegang krijgen tot je laptop en alle bestanden. Gebruik nooit een openbaar wifi-netwerk zonder VPN als je met de bedrijfslaptop elders werkt of in de trein zit.

8 **Herken hackers en oplichters.**

Hackers en oplichters gebruiken vaak trucs om toegang te krijgen tot je data. Kwaadwillenden kunnen zich bijvoorbeeld voordoen als IT-medewerkers en zo per telefoon om inloggegevens vragen. Ga daar nooit op in of neem eerst contact op met je eigen IT-bedrijf.



9 **Wees alert op phishing e-mails**

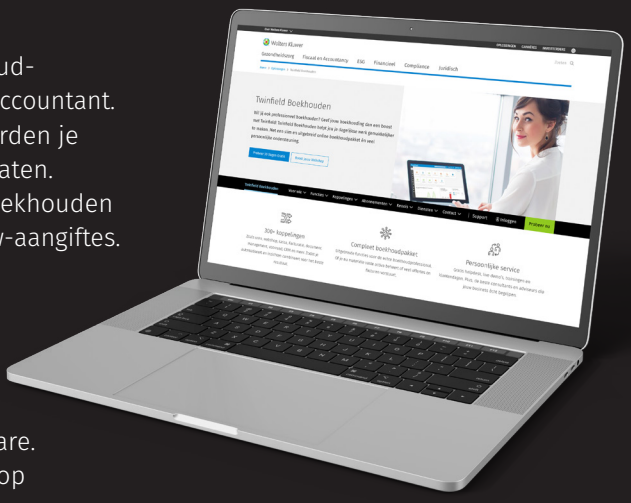
Phishing e-mails zijn allang geen knullige teksten meer vol taalfouten. Ze zien er vaak heel professioneel uit en lijken afkomstig van bedrijven als Apple of ING. Als je de afzender van een mail niet kent of de mail ziet er verdacht uit: klik dan NOOIT op de links. Wees ook alert als men om geld of gegevens vraagt of als het verzoek spoed heeft. Open in geen geval bijlagen en voer nooit inloggegevens in via een link uit de e-mail. Vraag je werkgever eventueel om een online training te volgen.

10 **Gebruik geen (onbekende) USB-sticks.**

Steek nooit een onbekende USB-stick in je computer. Als er een wordt gevonden, laat hem dan onderzoeken door de IT-afdeling, als die er is. Inbreken via een USB-stick is een methode die veel hackers gebruiken.

Deze tips worden je aangeboden door Twinfield

Twinfield Boekhouden is een professioneel en compleet online boekhoud-programma, waarmee je slim en gemakkelijk online samenwerkt met je accountant. Twinfield Boekhouden koppelt met bijna alle webwinkelsoftware. Zo worden je verkopen eenvoudig geregistreerd en heb je actueel inzicht in de resultaten. Je gegevens zijn zeer veilig en je werkt volledig in de cloud. Twinfield Boekhouden werkt ook goed bij grote aantallen transacties en helpt je bij foutloze btw-aangiftes.



Over Wolters Kluwer

Wolters Kluwer is een van de grootste aanbieders van informatie, software, tools en diensten voor juridische en fiscale professionals. Wereldwijd werken honderdduizenden van hen elke dag met onze software. Voor hun dagelijks werk vertrouwen zij op onze jarenlange expertise en op onze producten. De divisie Tax & Accounting levert professionele software, waaronder Twinfield Boekhouden, Twinfield Samenwerken, Alure Online, Basecone en Avanzer Aangifte.

Contact

Twinfield | De Beek 9-15
3871 MS | Hoevelaken | The Netherlands
www.twinfield.nl | +31 (033) 467 70 10

Wolters Kluwer

←