

THUIS VEILIG INTERNETTEN



ICTKeurmerk

WWW.ICTKEURMERK.NL

INLEIDING

Internet is niet meer weg te denken uit het dagelijks leven. Sinds de introductie ervan is er dan ook veel veranderd en de mogelijkheden worden steeds groter. Veel aankopen worden tegenwoordig online gedaan en ook financiële zaken gaan via het internet, zoals internetbankieren. Maar internet kent ook een keerzijde. Internetcriminaliteit neemt toe en criminelen worden steeds inventiever. Op verschillende manieren weten zij geld of persoonsgegevens te ontfutselen.

Een klein risico? Informeert u maar eens in uw omgeving hoe vaak het iemand is overkomen dat datagegevens verloren zijn gegaan. U zult schrikken van de uitkomst. Het kan iedereen gebeuren, net zo goed als internetcriminaliteit. Daarom is het van belang dat u uw ICT-apparatuur optimaal beveiligd heeft. U bent op de goede weg door een Keurmeester van het ICTKeurmerk in te schakelen, maar hoe moet het nu verder?

In "Thuis veilig internetten" leest u bruikbare tips en stappen die u kunt uitvoeren zodat u veilig blijft internetten. Veel voorkomende problemen worden uitgelegd en hierbij wordt vermeld hoe u deze problemen kunt voorkomen. Want voorkomen is altijd beter dan genezen.



ICTKeurmerk

INHOUD

Internetfraude Wachtwoorden Identiteitsfraude Smartphone & tablet Checklist

Dit is een uitgave van ICTWaarborg.

Bezoekadres

ICTWaarborg
Tasveld 1A
3417 XS Montfoort

Redactie

Gerrit Jan Bel, Kicky Tuit

Grafische verzorging

Haarsma Media, Leeuwarden



ICTWaarborg



INTERNETFRAUDE

Er zijn vele manieren van internetfraude. We zullen ons hier beperken tot de meest voorkomende.

Malware

Malware is schadelijke software die vijandige, schadelijke of irritante software op uw computer installeert. Internetcriminelen ontwerpen deze software zodanig dat deze een computer kan infiltreren, zonder dat de gebruiker dit merkt. Malware kan geïnstalleerd worden via e-mail, afbeeldingen of links op websites.

Cyber- en typosquatters

Deze vormen van internetfraude hebben met elkaar te maken, en overlappen deels. Bij cyber- en typosquatters veranderen internetcriminelen de domeinnaam (naam van de website, bijvoorbeeld www.ictkeurmerk.nl) van een website. De domeinnaam wordt vaak veranderd in een bekende naam, maar dan net iets anders

gespeld. Een voorbeeld is www.iphone.com, de enige echte site van Apple. Er bestaan talloze andere websites, zoals www.iphone.nl, die claimen de echte te zijn. Wanneer u naar deze site surft, kan er ongemerkt diverse malware op uw computer geïnstalleerd worden. Bij een typosquatter maakt u zelf een typefout in een domeinnaam. U komt daardoor op een andere site terecht, die fungeert als doorlink-pagina. U wordt doorgelinkt naar een andere pagina, die niet pluis is. Vervolgens kan uw computer geïnfecteerd worden met diverse malware.

Wat kan ik doen?

Let goed op welke websites u bezoekt. Twijfelt u of u een echte site bezoekt? Dan kunt u altijd een domeincheck doen. U checkt dan of het domein van de website daadwerkelijk geregistreerd is. .nl-domeinen kunt u checken bij de Stichting Internet Domeinregistratie Nederland (SIDN).

E-mailfraude

Bij het ontvangen en versturen van e-mail kan veel mis gaan. Zo kan u, bij één typefout in het e-mailadres, al privégegevens versturen naar een internetcrimineel. Ook kunt u diverse e-mails ontvangen die alleen maar als doel hebben u gegevens te ontfutselen. Er kan gevraagd worden naar codes, maar ook of u een bepaalde website wil bezoeken. Kijkt u op die link, dan is het mogelijk dat malware op uw computer geïnstalleerd wordt.

Wat kan ik doen?

Wanneer u een e-mail niet vertrouwt, let dan goed op spelling. Wordt er wel correct Nederlands geschreven? Ook kunt u de links, die u naar een bepaalde website willen sturen, controleren door er met de muis op te gaan staan. Er verschijnt dan in beeld naar welke website u gestuurd wordt. Het is altijd beter om een link over te typen in uw browser. Twijfelt u nog? Dan kunt u de organisatie van waaruit de e-mail ver-

stuurd is, ook bellen. **Let op: een bank vraagt u nooit om wachtwoorden, codes, nummers of pincodes.** Krijgt u toch een e-mail waarin uw bank vraagt om deze gegevens? Neem dan direct contact op met uw bank.

Phishing

Phishing is waarschijnlijk de meest bekende vorm van fraude. Bij phishing probeert een crimineel op een slinkse wijze gegevens van u te ontfutselen. Phishing gebeurt zowel via e-mail als de telefoon, of zelfs in combinatie. De criminelen proberen altijd belangrijke gegevens in handen te krijgen, zoals codes die gebruikt worden bij het internetbankieren.

Wat kan ik doen?

Uw bank, uw internet- en e-mailprovider en andere organisaties zullen nooit om codes, wachtwoorden, nummers of pincodes vragen! Geef deze daarom nooit weg, maar houd ze altijd voor uzelf.



WACHTWOORDEN

Een sterk wachtwoord is ontzettend belangrijk. Veel verschillende websites vragen om een wachtwoord, zoals Facebook, uw e-mail en ga zo maar door. Niet voor niets dient u hier een wachtwoord in te voeren: het is de bedoeling dat anderen niet bij uw persoonlijke gegevens kunnen. Het is daarom ook van belang voor een sterk wachtwoord te kiezen. Maar hoe doet u dat?

Er zijn verschillende manieren om uw wachtwoord sterk te maken. Er wordt aangeraden om gebruik te maken van hoofdletters, kleine letters, cijfers en tekens. Maar hoe onthoudt u uw wachtwoord dan nog? Daar is een simpel truckje voor. Neem een simpele zin, zoals: 'Jan ziet dat het 3 uur is.' U neemt van ieder woord de eerste letter. Het wachtwoord wordt dan: Jzdh3ui. U houdt de hoofdletter van Jan en het cijfer 3. Het wachtwoord is nu al behoorlijk sterk, maar u kunt er ook voor kiezen om tekens toe te voegen. Zo kunt u de 'i' vervangen

door een uitroepteken. Het nieuwe wachtwoord wordt dan Jzdh3u!. Een sterk wachtwoord, dat niet zomaar geraden wordt door een crimineel. Een andere truc om een sterk wachtwoord te bedenken en dit ook te kunnen onthouden, is het gebruiken van een boek. Neem de eerste zin van een hoofdstuk, en zet deze om in een sterk wachtwoord zoals hierboven is uitgelegd. Dit kunt u met iedere eerste zin van ieder hoofdstuk doen. Zo heeft u al snel een aantal verschillende wachtwoorden. Weet u een wachtwoord niet meer? Dan kunt u in het boek kijken.

6 belangrijke tips bij het bedenken van wachtwoorden.

1. Zorg voor een wachtwoord van minimaal 8 karakters. Hoe langer, hoe beter.
2. Verander regelmatig al uw wachtwoorden. Met regelmatig bedoelen we niet iedere week, maar tenminste één keer per jaar.
3. Houdt uw wachtwoorden veilig. Laat geen blaadjes met daarop uw wachtwoord rondslingeren bij uw computer, maar bewaar ze op een andere plek. Maak ook zeker geen bestand op uw computer met de titel 'wachtwoorden'.
4. Neem altijd een wachtwoord dat bestaat uit cijfers, letters en tekens. Deze wachtwoorden zijn het moeilijkst te kraken door criminelen.
5. Laat wachtwoorden niet automatisch onthouden door uw browser.
6. Gebruik verschillende wachtwoorden.



IDENTITEITSFRAUDE

Identiteitsfraude is het opzettelijk gebruiken van valse identificatiemiddelen. Bij identiteitsfraude geeft iemand zich uit voor een ander. Voor criminelen is het niet moeilijk om identiteitsfraude te plegen, ze hebben er slechts een paar gegevens voor nodig. Uw burgerservicenummer en naam zijn soms al voldoende. Identiteitsfraude is vaak zeer hardnekkig en het is niet altijd makkelijk aan te tonen dat u niet verantwoordelijk bent voor de bewuste handelingen.

Hoe herkent u identiteitsfraude?

- U ontvangt rekeningen die aan u zijn gericht voor spullen of diensten die u niet besteld heeft.
- U ontvangt brieven van advocaten of incassobureaus en deurwaarders waar u niets van weet.
- Op uw bankafschriften staan uitgaven die u niet herkent.
- Uw gebruikelijke rekeningen worden niet meer bezorgd.
- U staat bij de gemeente onder een ander adres ingeschreven.
- U kunt geen lening krijgen door een onbekende BKR-signalering.
- U ziet een of meer onbekende werkgevers op pensioen- of belastingoverzichten.

Wat kan ik doen?

- Wees altijd alert. Geef nooit wachtwoorden of persoonlijke gegevens aan onbekenden.
- Bewaar documenten met persoonlijke informatie altijd op een veilige plaats.
- Heeft u kopieën met daarop persoonlijke gegevens op uw computer staan? Scherm dan het burgerservicenummer af, door het bijvoorbeeld zwart te maken.
- Denk goed na over wat u op internet zet over uzelf.
- Geef niet snel een kopie van uw paspoort of identiteitsbewijs af. Vaak is het genoeg om uw paspoort of identiteitsbewijs te laten zien. In enkele gevallen is het wettelijk verplicht een aantal gegevens van uw paspoort of identiteitsbewijs over te nemen. Banken, notarissen en casino's zijn bijvoorbeeld verplicht de identiteit van hun

klanten vast te stellen. Bij het overnachten van een hotel hoeft geen kopie te worden gemaakt.

- Verhuisd? Breng relevante organisaties hiervan op de hoogte.
- Controleer regelmatig uw bankafschriften.
- Vernietig documenten met persoonlijke gegevens voordat u ze weggooit. Denk hierbij aan bankafschriften, hypotheekpapieren, ingevulde formulieren en alle brieven waar uw naam en adres boven staan.
- Verander uw wachtwoorden regelmatig.

Wanneer u toch slachtoffer wordt van identiteitsfraude, moet u al het bewijsmateriaal bewaren. Identiteitsfraude kunt u melden bij het Centraal Meldpunt Identiteitsfraude (CMI).



SMARTPHONE & TABLET

9 tips om uw smartphone en tablet te beveiligen.

Beveilig niet alleen u computer goed, maar ook uw smartphone en tablet. Ook via deze apparaten kunnen criminelen toegang verkrijgen tot uw persoonlijke gegevens.

1. Wees altijd alert. Ontvangt u rare meldingen die u niet vertrouwt? Neem dan contact op met de desbetreffende organisatie.
2. Zet een antivirusprogramma op uw smartphone en tablet. Er zijn er diverse. Ook gratis versies. In de app- of playstore kunt u zoeken op 'antivirus'. Een goede, gratis versie is de 'AntiVirus GRATIS' app van AVG Mobile.
3. Installeer altijd alle updates die uw smartphone of tablet aangeeft. Op deze manier zorgt u ervoor dat uw apparaat up-to-date blijft.
4. Gebruik een pincode of wachtwoord. Het liefst een pincode of wachtwoord van

meer dan 5 cijfers en/of letters.

5. Heeft u gebruik gemaakt van een internetbankieren-app? Vergeet dan niet uit te loggen.
6. Maak alleen gebruik van WiFi wanneer u zeker weet dat deze verbinding beveiligd is.
7. Kijk om u heen. Bankier niet overal. Criminelen kunnen met u meekijken terwijl u uw wachtwoord invoert. Risicovolle plekken zijn bijvoorbeeld internetcafés, koffiezaakjes, het station of in de trein.
8. Gebruik geen andere smartphone of tablet. Gebruik alleen uw eigen apparaten wanneer u gaat internetbankieren.
9. Volg het nieuws op het gebied van fraude.

CHECKLIST



11 tips die u helpen om veilig te internetten

1. Wees altijd alert! Vertrouwt u iets niet? Neem dan contact op met de desbetreffende organisatie.
2. Check altijd 'https' en certificaat en kijk goed op welke website u zich begeeft. Controleer of het webadres begint met https://. Klopt dit? Dan is de verbinding versleuteld en kan deze niet worden afgekeken. Ook kunt u het 'certificaat van echtheid' opvragen, door op het slotje in de adresbalk te klikken. Hier kunt u zien of de website ook bij de desbetreffende bank hoort.
3. Klik nooit zomaar op een link. Controleer links door de muis boven het linkje te laten zweven. U ziet dan het webadres waar de link heen leidt.
4. Kies voor sterke wachtwoorden.
5. Open geen onbekende bestanden of 'vage' websites.
6. Organisaties zoals uw bank vragen nooit om uw wachtwoorden, codes, nummers of pincodes. Houd deze dus altijd geheim!
7. Verstrek ook geen andere persoonlijke informatie.
8. Let op taal- en spellingfouten.
9. Controleer regelmatig uw bankafschriften.
10. Laat regelmatig uw computer scannen door de virusscanner.
11. Volg het nieuws rondom fraude.
12. Bent u toch slachtoffer geworden? Meld dit dan direct bij de desbetreffende organisatie!

En tot slot: laat uw ICT-apparatuur ieder jaar checken door een Keurmeester. U weet dan zeker dat uw apparatuur maximaal beveiligd is.

Het internet. Een bron van informatie en te gebruiken voor bijna alles. We gebruiken het dagelijks voor het versturen van e-mails, het lezen van nieuws, het kopen van nieuwe spullen maar ook veelvuldig om onze financiële zaken te regelen. Er kleeft echter een keerzijde aan het gebruik van internet. Internetcriminelen proberen op allerlei manieren uw persoonlijke gegevens te stelen en daarmee uw rekening te plunderen.

U bent al goed op weg door een Keurmeester in te schakelen, maar u kunt zelf ook een aantal eenvoudige stappen doorlopen om veilig te blijven internetten.

In "Thuis veilig internetten" leest u bruikbare tips en stappen die u kunt uitvoeren zodat u veilig blijft internetten. Veel voorkomende problemen worden uitgelegd en hierbij wordt vermeld hoe u deze problemen kunt voorkomen. Op deze manier bent u optimaal uitgerust tegen online bedreigingen.



ICTKeurmerk

www.ictkeurmerk.nl

ICTKeurmerk is een initiatief van ICTWaarborg